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

Special Report - Memphis, part 2

1/1/2011 - 8/26/2014

Security Privacy Ticket Number:	PSETS0000092188
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	7/17/2013
Date Closed:	7/25/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Veteran reported to PO that on June 10, 2013, his fiance called on telephone and spoke to a VA employee at the Emergency Department staff , and requested to know if he (veteran) has been to the VA hospital on that day. According to Veteran, his fiance provided his full name and last four of SSN employee who reviewed his health record and provided information on recent hospital and clinic visits to the fiance. Veteran stated that though he had been to the VA hospital on the day in question, the VA staff had no authority to disclose information about his hospital appointment and clinic visits to someone who is just a fiance and had no Power of Attorney or any legal right to have access to his health information . When PO asked Veteran about how he became aware of the disclosure , he replied that his fiance told him about it and then used the information he obtained to question his movement. PO requested phone number and name of the fiance for follow up on this incident but Veteran declined to provide such informaiton for fear that this will lead to a quarrel between them which will not be in his best interest.

Resolution

PO has concluded follow up on this complaint. Complainant declined to provide contact phone number for follow up with the informant so it was difficult narrowing down fact-finding investigation to specific VA employee(s). However, PO addressed issue with ER Nurse Manager and ER Supervising MD who in turn discussed the incident with ER staff. Both supervisors drew staff attention to policies and guidelines regarding release of information over telephone , especially in scenarios when callers claim to be Power of Attorney, Next-of-Kin or relatives of the patient. PO could not valid this complaint and, as such, no PII or PHI was compromised.

Complaint is considered closed as of 7/25/2013 with no further action required. PO will notify complainant about outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000092507
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	7/25/2013
Date Closed:	7/29/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A VA employee, also a Veteran, stated that on July 17, 2013 she had doctor's appointment at the VAMC. While she was waiting in her car at the patient parking lot one of the VA Police Officers approached and questioned her about her reason for using VAMC patient parking . Complainant stated she explained to the Police Officer about her scheduled doctor's appointment but the officer did not believe her so he went back to the Police Service to verifiy about her sheduled doctor's appointment. Complainant believes that the Police Officer had no right to verify about her doctor 's appointment and that this is a violation of her personal privacy.

Resolution

PO has concluded his fact-finding on the incident. A VA employee, also a Veteran, was unhappy about a VAMC Police Officer who verified her clinic appointment in the system. Employee parked at the VAMC patient parking lot and the Police Officer questioned her about the use of patient parking . In her response, employee stated she had clinic appointment. Employee insisted that the VA Police Officer has violated her personal privacy for accessing her clinical record to verify her doctor's appointment.

It was revealed that the Police Officer notified his supervisor (who has limited access to patient health record) to verify to confirm whether or not the employee had clinic appointment on that day. It turned out that the employee had clinic appointment in the afternoon of that day. The Police Supervisor clarifed that the confrontation would have been de-escalated if the Police Officer had believed the employee's story and excused her to use the parking space.

PO noted that there was no violation arising from this incident and that no PI or PHI was compromised.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000092893
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	8/2/2013
Date Closed:	8/13/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0595166
Date US-CERT Notified:	8/2/2013
US-CERT Case Number:	INC000000303214
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	No
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

On 08/01/13, an employee (Psychologist) met with a VA patient between 3:00 PM and 4:15 PM. At the conclusion of the session, both patient and provider agreed to meet again in the next three weeks. Provider recorded next meeting schedule in his daily Personal Planner (book) which he keeps purposely to track Veterans appointment and other patient care activities. When Provider concluded the session, he stepped outside his office briefly. Patient also left for home. Upon returning to his office, provider decided to reach out to pick his daily planner but could not find it anywhere in the office. At 6:15 PM, Provider then called the patient to inquire if he had accidentally taken the daily planner. Patient requested to allow him to search and then call him back. Patient noted he accidentally placed the provider's daily planner in his 3-ring binder he carried with him for the clinic session with the provider. He then called and notified the provider about it. Provider drove to patient's home to pick up and secured the planner his office. Patient explained to provider that he accidentally picked the daily planner and was not aware that it was kept in his 3-ring binder until he began to search through his belongings. Patient assured the provider that he never looked into it and so does not know the kind of information that is kept in there. Provider described daily planner as: "Planner 2013 - At a Glance #70-950." This is his personal daily planner he has been using to keep patients appointment and other sensitive information he maintains as reminders. During a short telephone between PO and Provider, he stated that the names in the daily planner will be around 40, and this includes Veterans' full names and their last four digits of the SSN. The Provider realized that the planner was missing around 4:15 PM and retrieved it from patient around 6:15 PM. The Privacy Officer (PO) will contact the Provider on Monday, 08/05/13 to determine the exact number of Veterans affected by this incident.

Incident Update

08/06/13:
PO has concluded his fact-finding on the incident. The PO, the Provider, Provider's Supervisor and Vice President of the Local AFGE were in attendance for the fact-finding. The Provider (Psychologist) admitted keeping a personal daily planner which he uses to track patient appointments. He admitted the only PII he keeps in the daily planner is patient full name and last four digits of their SSN. The Provider reviewed the daily planner and noted there are 159 Veterans affected by this incident.

As part of the resolution process, the PO requested Chief of Mental Health Service to address this incident in the Mental Health Staff meeting held yesterday (08/05/13) at 2:00 PM. The Chief re-educated all staff during the meeting regarding use of personal logbooks and daily planners. The Chief also requested staff to stop using daily planners immediately to prevent potential privacy breach.

During the fact-finding, the PO determined that there is no indication to show that patient accessed information (PII) contained in the daily planner since he was not aware that he had it in his 3-ring binder. The patient became aware of the daily planner only when the Provider called to speak with him and requested him to search his personal belongings for it. Patient has been very cooperative and assured provider that he did not look into the daily planner at all.

Resolution
PO has concluded his fact-finding on the above ticket and need assistance in closing the it. As PO explained in the resolution comments, there is no indication that the PII (that is patient name and their last four of SSN) were compromised as the patient who accidentally took the daily planner was not aware that he had it in the 3-ring binder. When Provider discussed the issue with patient, he quickly went to his house to search through his belongings and then found the daily planner in his 3-ring binder. Patient apologized to provider and stated that since he was unaware the daily planner was in his possession, he had no knowledge about the information contained in it.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000093131
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	8/8/2013
Date Closed:	8/12/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An ER patient is complaining that the SSN on patient armband poses a privacy risk. Her concern is that anybody using a smart phone or other mobile devices can easily scan the armband and retrieve the embedded personally identifiable information. She also has concern about lack of patient education on armband usage especially SSN and other ID that are embedded on the armband. In her opinion, if Veterans received patient education on armband usage, there would not be any complaint about it.

Resolution

During the fact-finding, PO met with the team leader of the committee overseeing the implementation of new patient armsband which contains their full SSN, full name and photo. She explained that SSN on the armsband is required by VA for patient care and also to avoid medical errors. She stated that this is a decision taken by the VA Central Office and that the medical center has no control over it. PO and the team leader are teaming up to develop patient education materials to raise patient awareness regarding the sensitive nature of the armband and its role in pateint safety.

Case is closed as invalid; complainant will be notified by PO regarding the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000093242
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	8/12/2013
Date Closed:	10/2/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A daughter of a VA patient reported to PO that her father received an orthopedic clinic follow up appointment letter from the VA , but her father has never been seen at the ortho clinic for any reason. Complainant stated this is a violation of her dad's privacy because the clinic may have provided his IIHI (individually identifiable health information) to a provider(s) who will have nothing to do with his health information. Complainant requested the Memphis VAMC to intestigate this issue. PO requested daughter to mail the clinic appointment letter for review to identify the VAMC staff who may have schedule this patient appointment by accident.

Resolution

The Supervisor responsible for the outpatient clinic conducted a fact-finding into the complaint and met with the employee who mailed the letter with another Veteran’s clinic appointment reminder letter. Supervisor re-educated employee on certain key elements of her job requirements especially protecting and safeguarding VA patient information when preparing correspondence for mailing. Supervisor also issued written counseling to employee to avoid future occurrence of this incident. Complaint is considered closed as of today, 10/2/2013.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000093330
Incident Type:	Unauthorized Electronic Access
Organization:	VISN 09 Memphis, TN
Date Opened:	8/14/2013
Date Closed:	8/14/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0595596
Date US-CERT Notified:	8/14/2013
US-CERT Case Number:	INC000000305902
Category:	Category 4- Improper Usage
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A VA employee sent an unencrypted email message containing a screen shot of the full Social Security number and name of one VA Provider to VetPro Help Desk email group. The email group is outside of VA network. The mail group is comprised of 10 VA staff and one non-VA staff (NIH system administrator). The VA employee does have valid PKI certificates assigned. The responsible ISO will be notified via Remedy Ticket and email.

Incident Update

08/14/13:
The email was sent to the intended recipients. No data breach occurred.

Resolution

I informed the VA employee to importance of PKI and it used and provided on-site training to the VA employee on how to set-up the encryption option in email to remain ON during all e-mail especially VET PRO data. I informed the VA employee that the option can be turned off, when no VA sensitive data is being transmitted. The employee stated she will comply.

No further action taken by the ISO, request ticket to be closed.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000093432
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	8/15/2013
Date Closed:	10/23/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0595697
Date US-CERT Notified:	8/15/2013
US-CERT Case Number:	INC000000306492
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Veteran A received a letter to complete a means test. Included in the envelope was an appointment request for Veteran B. It contained Veteran B's name, address, and appointment information.

Incident Update

08/16/13:
Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

The mail operation staff has been counseled to exercise due diligent when preparing correspondence for mailing. In order to prevent future occurrence, the mail operation staff has been instructed to update the mailroom equipment and service agreement. This will entail standardized cleaning and servicing schedules to ensure proper operation and calibration. Replacement equipment with up to date soring and metering will be procured to ensure higher percentage of accuracy

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000093608
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	8/20/2013
Date Closed:	8/22/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0595863
Date US-CERT Notified:	8/20/2013
US-CERT Case Number:	INC000000307712
Category:	Category 4- Improper Usage
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An OI&T employee went to replace a contingency computer which contains patient information . This computer is used in times of power or network outages. The procedure is that when there is an outage, a nurse manager will go get the contingency book which should be located in a locked location, like a locker or file cabinet. Then the nurses have directions on how to log into the computer using a username and password that has been set up on this computer to be used to log into the computer. When the OI&T employee went to remove this computer he noticed that the user name and password was written on a yellow sticky paper and taped on top of the computer. This information is very sensitive and cannot be displayed in such a manner. He then realized it was his duty to report this incident. So he notified the Privacy Officer and Information Security Officer (ISO).

The Privacy Officer also notified the ISO of the incident and provided the yellow sticky note that was taped to the computer . The note contains the logon username and password (handwritten) for the medical contingency workstation. The ISO is currently conducting fact-finding. Contingency workstations are encrypted.

Incident Update

08/22/13:
The contingency computer was located in the Nurses' Room. The room is attended by nurses at all times, otherwise room is locked when unattended. This was a policy violation, not a data breach.

Resolution
Upon ISO fact finding the following has been determined:
1. Contingency workstation is located in nurse's room with other computers. This room is always attended by staff when door is open; otherwise room is locked.
2. The username/password found is not the current logon to access the workstation.
3. Upon nurse's logging onto contingency workstation, to use applications (BCMA Backup, Health Summary) they must enter their own individual access/verify codes for authentication in order to access patient information.
4. Nurse Manager covers topics during staff meetings: process for logon to workstation and securing room.
5. ISO met with nursing staff working in this area to gather info and provided continuous education. Covered the following:
   a. securing all log on credentials
   b. not sharing log on credentials
   c. not posting log on credentials
   d. never leaving workstations unattended while logged on
   e. securing all forms of information

No information was at risk of compromise due to the written logon codes found because this is not the current codes for logon to the contingency workstation; codes had previously been changed by OI&T. In order to access patient information users must enter their own individual access/verify codes for authentication. ISO and PO are currently attending staff meetings for all services to educate them on protecting sensitive information.

Request closure of this incident.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000094054
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	8/30/2013
Date Closed:	8/30/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0596285
Date US-CERT Notified:	8/30/2013
US-CERT Case Number:	PSETS0000094036
Category:	Category 1 - Unauthorized Access
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

On 8/30/13, an OIT employee of the hardware section reported a USB drive used for the Windows 7 migration was lost. The following information has been determined during the Information Security Officer (ISO) fact-finding:

1. Is it encrypted? No
2. What is stored on the USB? Windows 7 image
3. Any PII, PHI, SPI? No
4. Circumstances surrounding how it was lost? USB was not in the room when employee when back to collect it.
5. What safeguards were in place to protect the USB? password protected
6. When was it discovered missing? 8/30/13
7. Was it left unattended over night? no
8. What location? 1E120
9. Was room locked? yes
10. Who has access to the password? OIT hardware
11. Is there a waiver for the unencrypted USB? If not, what approval process is in place to use these for updates? Win 7 USB Waiver approved and uploaded.
12. When was the last time the USB was seen/used by OIT? about a week ago
13. Have you asked staff in that area about the USB? yes
14. Why has there been a week delay in reporting this incident? trying to locate device
15. Can you be more specific as to when the device was first noticed as missing (date/time)? cannot, do not remember
16. Was it reported to anyone at the time of discovery? yes, team lead

Incident Update

08/30/13:
No data breach has occurred. There was no sensitive patient data on the thumb drive.

Resolution
The following information has been provided to OI&T employee, hardware team lead, FCIO, network supervisor:

VA Handbook 6500.2/1
8. EQUIPMENT
a.It is VA policy that VA facilities, contractors, and BAs will report in a timely manner all lost, stolen, or missing IT equipment that may be used to store, transmit, create, access, duplicate or copy, disclose or use SPI, whether it is encrypted or unencrypted. Examples of covered IT equipment include laptops, workstations, thumb drives, hard drives, routers, USB device, PDA, Smart phones, blackberry device, I-Pad, and other similar devices. VA must report this unaccounted for, stolen, or missing equipment to Congress, even if VA determines that the devices do not contain SPI. VA does not have to report to Congress any lost, stolen, or missing equipment if VA determines that any storage capability on the equipment was encrypted with an encryption application approved by the Office of Cyber Security (OCS), but missing equipment is still reportable to VA upper management.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000094281
Incident Type:	Non-VA Responsible/Non-Incident Upon Further Investigation
Organization:	VISN 09 Memphis, TN
Date Opened:	9/5/2013
Date Closed:	11/1/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An EMS employee felt sick and was taken to the VAMC Emergency Room for treatment. According to the complainant (EMS employee) the ER Provider called to notify his immediate supervisor that he was being treated at the ER. Complainant stated that when he was released from the ER to the floor, his supervisor wanted to send him home for no reason. He requested his supervisor to provide his reason for sending him home but he declined to do so. Complainant feels that the ER provider has violated his personal privacy by notifying his Supervisor that he was being treated at the VAMC ER .

Resolution

PO investigated complainant's allegation:

That his supervisor obtained information about his medical condition without his permission or need to know when he became ill at work and was taken to the ER for treatment.

During PO's meeting with the Supervisor, he clarified that complainant was found drunk at Memphis VAMC so VA Police escorted him to the ER Supervisor narrated that his immediate Boss instructed him to go to the ER to speak with complainant and possibly pick up his car keys from him for safe keeping. PO's review of Memphis VA Police Uniform Offense Report (UOR) confirmed supervisor's statement. The UOR report indicated complainant was drunk and this was not a hidden incident. While at the ER to see complainant, the supervisor determined he (complainant) would not be able to work for the rest of his tour of duty so he asked him to go home.

After review of the UOR report, PO determined that there was no evidence of violation. Supervisor therefore acted in the best interest of the complainant and the agency. Complaint is considered closed as of 10/31/2013; complainant will be notified about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000094285
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	9/5/2013
Date Closed:	9/25/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0596516
Date US-CERT Notified:	9/5/2013
US-CERT Case Number:	INC000000311570
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

A VA patient reported to PO that someone has changed his mailing address in his VA records and this has resulted in his medication being mailed to another patient (Veteran). Complainant stated that the recipient of his medication (i.e. the other Veteran) called to notify him that he has received medication in error - through his home address. Complainant stated that he then called the VA to verify for his current address the VA has in the system. According to the complainant, the VA staff was to call him back to provide the requested information but failed to do so.

PO requested the complainant to verify his mailing address; the address provided is different than what is in his CPRS record. PO will follow up on this incident tomorrow.

Incident Update

09/06/13:
Patient A will be sent a notification letter.

Resolution
Supervisor met with the employee whose action resulted in this breach. It was determined that the error occurred when a VAMC employee was performing pre-registration assignment and inadvertently updated the address and Next-Of- Kin information pertaining to the complainant with another Veteran's data. Their Supervisor who oversees the department has met with and re-educated the employee on the proper use of pre-registration screen to avoid future occurrence of this type of incident.

Redacted copy of notification letter sent to the Veteran has been scanned and uploaded to this ticket in PSETS . This incident is considered closed as of 9/24/2013.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000094759
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	9/17/2013
Date Closed:	9/23/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

The wife of a Veteran reported to the Privacy Officer (PO) that she suspects two VA employees (Social Workers) have accessed her husband's medical records without appropriate permissions. She recounted her story saying her husband has transferred his VA care to Missouri VAMC and that they needed copies of his medical records to be forwarded to this VA hospital. On 08/28/13, she called to speak with one of the Social Workers to inquire if her husband 's medical records had been forwarded to Missouri are requested previously. She stated that the Social Worker became a little irritated and wanted to know about her husband medical problems. She considered this as inappropriate question and told her that was none of her business. Complainant stated that the Social Worker became more irritated and said, I can log in to the system and see it for myself.

Resolution

During the fact-finding PO determined that one of the two Social Workers mentioned in the complaint was less concerned about the issue , and should not have been connected with the complaint. The other Social Worker was performing her official VA duties by reviewing the Veteran 's medical records to ensure that appropriate "care-giver" documentation was released to another VA Medical Center where the Veteran was transferring his care . The wife of the Veteran was participated in VA care-giver's program and this required VA Social Worker's review of the Veteran's health records to validate the wife's participation in the program. According to the Social Worker, the wife was of the opinion that her involvement in the care giver's program had nothing to do with the review of her husband's health records so she accused the Social Worker for breaching her husbands personal privacy . PO determined that there was no evidence of a breach; the Social Worker was performing her officoal VA duties and had need-to-know reason for review the Veteran's health records. The complaint is closed as of 9/23/2013. PO will notify complainant regarding the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000094813
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	9/18/2013
Date Closed:	10/23/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0597016
Date US-CERT Notified:	9/18/2013
US-CERT Case Number:	INC000000314516
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	No
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Veteran A received an appointment letter for Veteran B that was mis-mailed to him.

Incident Update

09/19/13:
Veteran B will receive a HIPAA letter of notification.

Resolution

Mitigation: The mail operation staff has been counseled to exercise due diligent when preparing correspondence for mailing . In order to prevent future occurrence, the mail operation staff has been instructed to update the mailroom equipment and service agreement . This will entail standardized cleaning and servicing schedules to ensure proper operation and calibration. Replacement equipment with up to date soring and metering will be procured to ensure higher percentage of accuracy

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000094816
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	9/18/2013
Date Closed:	9/27/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

VA employee reported that her supervisor opened and read her personal (private) mail sent by her creditor through the medical center mailing address.

Resolution

A VA employee alleged that her Department Supervisor had tampered with her private mail and read the contents .
PO found complainant's statements to be inconsistent with personal statements provided by the Supervisor and the Assistant Supervisor who have been involved in delivering private mails to her at different occasions . Complainant insisted her Supervisor had opened and read her private mail on two occasions; however, she had no witnesses to prove the allegation. The Supervisor clarified that he has on two occasions counseled the complainant to refrain from receiving her private mails through the VA since the existing medical center mail policy prohibits employees from receiving private mails through the facility . PO verified and confirmed this statement in the medical center mail policy memo # 136-13, ie. DIRECT ACCOUNTABILITY FOR MAIL MANAGEMENT. PO, therefore, declared this complaint invalid. Complaint is closed as of 9/27/2013. Complainant will be notified in an official memo from PO's office regarding the outcome of this fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000094817
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	9/18/2013
Date Closed:	10/8/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0597018
Date US-CERT Notified:	9/18/2013
US-CERT Case Number:	INC000000314537
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	No
OIG Case Number:	N/A
No. of Credit Monitoring:	4
No. of Loss Notifications:	

Incident Summary

The medical center travel office mailed a travel voucher to a Veteran and mistakenly included travel vouchers belonging to four other Veterans . The Veteran called the medical center to notify the Travel Office that he received four travel vouchers in error . The supervisor over the Travel Office notified the Privacy Officer (PO) that the travel voucher contains the Veterans' full name, SSN, date of birth, address, etc.

Incident Update

09/19/13:
The four Veterans will receive letter offering credit protection services .

Resolution

Supervisor responsible for Travel and Eligibility Section has re-educated all staff about importance of protecting and safeguarding Veterans protected health information (PHI) at all times. In order to prevent future occurrence of this incident, the supervisor has created a process of double verification which will require envelopes and corresponding addresses to be reviewed twice to ensure their accuracy before being mailed.

It is believed that personally identifiable information on the travel vouchers may have been compromised so PO has mailed out the Credit Monitoring letters to the three Veterans affected by this incident. Redacted copy of the letter has been uploaded to PSETS. This complaint is considered closed as of 10/8/2013.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number: PSETS0000095590

Incident Type: Mishandled/ Misused Physical or Verbal Information

Organization: VISN 09
Memphis, TN

Date Opened: 10/7/2013

Date Closed: 10/11/2013

Date of Initial DBCT Review: N/A

VA-NSOC Incident Number:

Date US-CERT Notified: N/A

US-CERT Case Number: N/A

Category:

Date OIG Notified: N/A

Reported to OIG: N/A

OIG Case Number: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

A Veteran reported to Privacy Officer that the VA Memphis Travel staff has misplaced his two travel vouchers submitted about a month ago . He is concerned that his personally identifiable information such as full name and SSN may have been compromised.

Resolution

Chief, Patient Access and Enrollment investigated the complaint and met with employees assigned to the Travel Office . He noted the procedures for issuing Travel Vouchers for payment are properly and consistently followed by staff which safeguard and protect sensitive personal information . Thus, based on the proper procedures being followed at the Travel Office , it is unlikely the travel vouchers were tendered in for processing, and that it may have been mishandled elsewhere before the Veteran came to the Travel Office . Even though the Supervisor did not find any evidence that suggest staff mishandled the travel vouchers , he re-educated staff to closely monitor the travel voucher drop box to prevent unauthorized access to it .

Based on the summary report of the fact-finding, PO could not determine if complainant's PII was compromised. Complaint is considered closed as of 10/11/2013; PO will notify complainant's about the outcome of the investigation.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000095591
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	10/7/2013
Date Closed:	10/10/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Staff from the Memphis VAMC Human Resource Office sent an unencrypted email to an individual at the Office of Safety & Risk Awareness/ Credentialing and Privileging (10A4E) regarding a prospective VA employee who was being verified for VA employment in the VetPro system. The encrypted email contained full SSN of this prospective employee.

Resolution

PO met with HR VetPro staff and his supervisor to review the incident. Staff had active PIV card that could encrypt mesages successfully; PO noted he had not properly configured it to activate the encryption key. PO assisted to configure the PIV card and also provided assistance to staff to make sure he can send encrypted messages with his PIV card without any problems. Staff sent an encrypted message to himself which was successfully done.

Incident is considered closed as of 10/9/2013.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000095646
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	10/8/2013
Date Closed:	10/22/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0597844
Date US-CERT Notified:	10/8/2013
US-CERT Case Number:	INC000000318815
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Veteran A reported that he received his GI Lab result with Veteran B's GI lab result all combined on one sheet at his home address. The only Personally Identifiable Information (PII) which appeared on the Veteran B's GI Lab result is his home address.

Incident Update

10/08/13:
Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

PO has met with the employee and his supervisor to address all issues which resulted in this incident. Employee admitted his wrongdoing and provided assurance that the incident will not reoccur again in the future. PO and Supervisor went over the issues and explained to employee the consequences that may arise if proper attention is not paid how he reviews patient PII for official correspondence from his desk . PO determined that the only PII that have been inappropriately exposed which pertains to the affected Veteran was his full name and home address .

Complaint is considered closed as of 10/22/2013. PO will notify the Veteran who reported the incident about the outcome of the fact-finding and remediation measures the facility has put in place to avoid future occurrence of the incident.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number: PSETS0000095724

Incident Type: Mishandled/ Misused Physical or Verbal Information

Organization: VISN 09
Memphis, TN

Date Opened: 10/10/2013

Date Closed: 10/11/2013

Date of Initial DBCT Review: N/A

VA-NSOC Incident Number:

Date US-CERT Notified: N/A

US-CERT Case Number: N/A

Category:

Date OIG Notified: N/A

Reported to OIG: N/A

OIG Case Number: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

A Veteran reported to Patient Advocate that Paralyzed Veterans of America (PVA) staff divulged a private conversation he had with her to a group of Memphis VAMC employees. The complainant clarified that he discussed with the PVA staff about his wife pregnancy and that he was not expecting her to disclose this information to anybody.

Resolution

PO determined that the Memphis VAMC has no responsibility to investigate and address privacy complaints /breaches involving employees from the Paralyzed Veterans of America (PVA). PO will advise Veteran to contact the PVA leadership to investigate the complaint. Complaint is considered closed as of 10/11/2013.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000096241
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	10/25/2013
Date Closed:	11/8/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Medical Support Assistant at the Neurology Outpatient Clinic failed to secure/protect VA sensitive information during practice fire drill.

Resolution

PO met with employee to investigate her involvement in the complaint. Her Supervisor was invited to the fact-finding meeting. Employee admitted the allegation that “she failed to secure and protect VA sensitive information on her desk.” She explained that she is new at her work Unit, and has been with the VA about 7 months. She stated she is not very familiar with so many routines and protocols at the medical center. She explained further that on 10/18/2013, there was a fire drill at her work unit and the nearby Ward which was her first experience since she became Memphis VAMC employee. When the alarm sounded, she thought it was a real fire outbreak; she saw other staff running here and there so she became confused and left her work area without securing all the papers and other sensitive information she was working on. She explained that when the fire drill ended, she interacted with other staff and learned that it was not a real life situation but was a practice fire drill. She then went back to her work station to review all the records/documents she left behind. In her personal statement which she submitted via email, she admitted she has now become familiar with the routines and protocols at the VA and will do everything possible to secure VA sensitive information at all times. PO interviewed one of the co-workers regarding employee’s attitude towards privacy safeguards and protections within the work unit. She stated the only occasion the employee left VA sensitive information unsecured was the day they had a fire drill. Employee’s supervisor counseled her during the fact-finding meeting to be mindful to protect VA sensitive information provided to her during her tour of duty.
PO determined that though the employee failed to secure VA sensitive information during the fire drill, her actions did not result in any PII/PHI being compromised. Complaint is considered closed as of 11/7/2013

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000096246
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	10/25/2013
Date Closed:	11/1/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Program Support Assistant reported that her supervisor has obtained copy of her personal sensitive information without need to know . She submitted her FMLA paperwork about her daughter's medical condition to the Human Resources Department and the supervisor requested a copy to keep on her (complainant) competency file in his office. She stated that during a meeting with the supervisor to discuss work related issues, she saw a copy of the FMLA paperwork in a folder he was holding. According to the complainant, after the meeting, the supervisor asked about the medical condition of her daughter. She stated the supervisor's question surprised her because she had not told him about her daughters medical problems. She feels the supervisor's action is a violation of her personal privacy and request him to be investigated.

Resolution

PO investigated complainant's allegation:

1) that, the supervisor has obtained and kept a copy of her Family Leave Medical Act (FMLA) paperwork in employee's competency folder. Complainant stated this is a violation of her personal privacy since the FMLA paperwork contains sensitive personal information.

During the fact-finding, Human Resource Department (HR) clarified that the department does not keep employees FMLA paperwork. Supervisors use FMLA paperwork to make decisions regarding employee family leave requests. In view of this, supervisors are permitted to keep FMLA paperwork to serve as reference when necessary.

2) that, the supervisor has violated her personal privacy by asking about her daughter's medical condition. When PO met with the supervisor during fact-finding, he confirmed asking the complainant about her daughter's health condition because she (complainant) previously told him about the medical problem the child was going through. This occurred when complainant asked for leave to go home to attend to her sick daughter. According to the supervisor, if complainant had not told him about the nature of her daughter's medical problem, he would not have had any knowledge about it. The supervisor is new to Memphis VAMC; he has been here less than 4 months.

Based on the outcome of the fact-finding, PO determined that there is no evidence of a violation. Complaint is therefore considered closed as of 10-31-2013. Complainant will be notified about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000097293
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	11/22/2013
Date Closed:	1/8/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

During an audit of an active VA Research Study, the Memphis VA Medical Center Research Compliance Officer (RCO) noted mailing addresses were collected for some of the enrolled subjects. Upon further review, he also noted the collection of mailing addresses was not specified by the research investigator in the signed HIPAA authorization and was also not listed in the PO and ISO Data Privacy & Security Checklist. The RCA noted 7 out of 35 subjects enrolled in the research study were affected. The RCA noted that the research investigator was approved per the HIPAA Authorization to collect email addresses and phone numbers but not study subjects mailing addresses. PO determined that the affected PII in this incident are: full name and mailing addressed of the enrollees.

Resolution

The ACOS/R restricted access to the pertinent files containing the sensitive information and the principal investigator (PI) and study staff no longer have access. The PI has submitted waivers for informed consent and HIPAA for that study and the amendment containing those documents will be reviewed at the January 22, 2014 meeting of the IRB. If approved, the PI and her study staff will be given access to the data.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000097522
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	11/29/2013
Date Closed:	12/13/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

During rounds on 11-27-2013, a supervisor from Business Office noted a Medical Support Assistant (MSA) had left his work area while his workstation was still logged into VistA and displayed VA patient sensitive information. The MSA is a check-in clerk assigned to this area - cardiology outpatient clinic. The work area is an open space that offers easy access to the public if the area remains unattended. When the supervisor arrived at the check-in desk, there was a VA patient standing in front of the desk looking for someone to assist him. According to the supervisor, information displayed on the computer screen was VA patient appointment data. He could not tell how long the MSA had been away from his workstation and also how many patients/Veterans had viewed information displayed on the screen. In order to secure the area, the supervisor remained there until the MSA showed up.

Resolution

PO met with the employee and his supervisor to resolve the complaint. Employee admitted stepping outside from his work area in a brief moment without logging his workstation off. During the fact-finding PO determined that during the time employee stepped outside his work area for about 3 minutes and during this time there was nobody in close proximity to his workstation. The Supervisor explained that the only patient who was in the check-in area was standing a few feet away and could not have seen any data displayed on the computer monitor. Based on this information, PO determined that there was no PII that could have been compromised as a result of the incident.

PO reviewed employee training records in TMS and noted he has completed VA Privacy and HIPAA Focused Training and also VA Privacy and Information Security Awareness and Rules of Behavior training. PO explained to employee the potential privacy risks in his behavior and advised that he should not allow the behavior to re-occur. Complaint is considered closed as of 12-13-2013.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000097548
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	12/2/2013
Date Closed:	12/23/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0599666
Date US-CERT Notified:	12/2/2013
US-CERT Case Number:	INC000000329849
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	28
No. of Loss Notifications:	1

Incident Summary

On Monday morning, 12/2/13, the Privacy Officer was notified via email by an employee stating on 12/01/13, a Resident was involved in a strong arm robbery at the Medical Center West parking lot at approximately 6:45pm. The Resident was going to her vehicle when she was approached by a black male with a gun. The suspect took her bag which contained her books, stethoscope, and an assignment list containing approximately 14 patient names and their last four digits of SSN. The robber made away with the bag and all its contents.

Incident Update

The Privacy Officer (PO) reports the Information Security Officer's report shows the Resident involved in the robbery has not been issued any VA laptops, as reported early. It has also been determined that there are 18 patients affected by the incident instead of 14 as reported in the initial notification PO received.

Therefore 18 Patients will receive a letter offering credit protection services.

12/04/13:
PO conducted a fact-finding into this incident today; met with the VA Resident, Chief of Medicine Service and Chief of Education Service who is also responsible for Graduate Medical Education program at the Memphis VAMC. PO is going to meet with ISOs to review outcome of the fact-finding and then provide appropriate remediation to prevent future occurrence of the incident among other Residents.

12/11/13:
need ten more CPS and one Next of Kin notifications.

Resolution
Privacy Officer and Information Security Officer have provided education to the Medical Center leadership It has been requested that residents provide a documented and signed authorization to take patient information outside of the hospital. PO and ISO recommend that the Medical Center leadership intervene to stop Resident/Providers from taking VA Sensitive information outside the hospital.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000097792
Incident Type:	Unauthorized Electronic Access
Organization:	VISN 09 Memphis, TN
Date Opened:	12/6/2013
Date Closed:	12/31/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0599904
Date US-CERT Notified:	12/6/2013
US-CERT Case Number:	INC000000331464
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A CBOC contractor quit on 11/15/13. The ISO, service and SDE were notified 12/3/13. The contractor's network account was terminated 12/3/13. The VistA account was accessed 12/6/13 after being placed in disuse status on 12/3/13. Unable to determine if this was system error or unauthorized access. ISO has asked the local VistA experts to check for last options/menus used and other events that may have occurred. VistA account has been terminated.

Incident Update

12/31/13:
This is not a security incident based upon information from the VistA managers.

Resolution

ISO received the following information from VistA Applications Specialist.
She is logging in from Jackson Mississippi VAMC using remote patient lookup. Every time someone accesses our system using remote capability (CAPRI for example) the last sign-on is updated. We have hundreds of remote users that log in from remote VAMCs and VBA.

File man inquiry shows. VISITED FROM: 586 SITE NAME: JACKSON VAMC

ISO has confirmed from COR for CBOCs that this person is a nurse practitioner at Jackson, MS VAMC.

Fact-finding concluded this is not an information security incident...no violation. Please close ticket.
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

12/27/13-----ISO has confirmed from COR for CBOCs that this person is a nurse practitioner at Jackson, MS VAMC.

Fact-finding concluded this is not an information security incident...no violation. Please close ticket.

PO agrees with ISO mitigation, there was no privacy incident.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000097859
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	12/9/2013
Date Closed:	12/10/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0599964
Date US-CERT Notified:	12/9/2013
US-CERT Case Number:	INC000000331823
Category:	Category 4- Improper Usage
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An employee from Ophthalmology reported to the Information Security Officer (ISO) that an Ophthalmology resident was telling another resident that he emails patient charts from CPRS to his personal email account.

The ISO met with the resident for fact-finding: 2-4 weeks ago resident stated that he created Word document and emailed DE-IDENTIFIED data to his personal email address of maybe 5-15 patients. This helps him stay abreast and follow-up with patient before their clinic visit. The Chief of the service informed him this practice cannot be done and he has stopped such practices. He now stays late or comes in early to review notes; creates Word document on desktop with last name & appointment time and other notes to assist him with patient care. He names the Word document with date. He then eventually deletes the document. He does not email data any longer.

The ISO advised the resident of the following: current process is acceptable. Resident must not email VA data or remove VA data outside of VA environment. Resident given copy of the Rules of Behavior to sign as a reminder of his responsibilities, and a printout of the ISO/ Privacy Officer (PO) information flyer for contacting ISO or PO and reporting incidents.

ISO contacted local IT staff to ensure permissions on resident desktop folder which is saved on a network drive is restricted ; confirmed.
Follow-up with service chief to remind residents of VA policies.

Fact -finding did not reveal disclosure of PII/PHI. Request ticket to be closed.

Incident Update

12/10/13:
There was a policy violation. No data breach has occurred.

Resolution
ISO advised resident of the following: Current process is acceptable. Resident must not email VA data or remove VA data outside of VA environment. Resident given copy of ROB to sign as a reminder of his responsibilities, and a printout of the ISO/PO information flyer for contacting ISO or PO and reporting incidents.

Follow-up with service chief to remind residents of VA policies.

Request ticket to be closed.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000098532
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	12/30/2013
Date Closed:	12/30/2013
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0600621
Date US-CERT Notified:	12/30/2013
US-CERT Case Number:	INC000000335685
Category:	Category 4- Improper Usage
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

12/30/13 VA Social Worker (SW) reported to the Information Security Officer (ISO) at the request of a program analyst for VHA NEPEC, that she sent an unencrypted email containing form VHA PRRC. The form is a program evaluation form published by the Northeast Program Evaluation Center as contracted by VACO. One form was sent unencrypted. One Veteran was involved. The form itself evaluates Veteran life satisfaction. SW was alerted this morning, December 30, 2013 at 0554 by NEPEC staff that the form was sent unencrypted. The form was originally sent to NEPEC. All persons are VA or VA Contracted employees. SW was advised by program analyst to recall message.

ISO advised SW, "In addition to recalling the message, please delete the unencrypted message, then also delete from your 'Deleted Items' basket. Examine each email before you send to identify whether it contains sensitive information, and encrypt the messages containing sensitive information. If you need assistance with encrypting messages please contact your service ADPAC or the ISO office."

SW states this was a mistake, she has PKI and used it to send other VHA PRRC forms that day. She also spoke with the ADPAC to review encryption process.

ISO provided SW with paper copy of ROB to read and sign; this has been completed. Also provided SW with definitions of VA Sensitive Information, PII, SPI, PHI, ROB. SW has completed all processes requested.

Please close incident.

Incident Update

12/30/13:
An internal unencrypted e-mail was sent. No data breach has occurred.

Resolution
No data breach has occurred.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000098772
Incident Type:	Unauthorized Electronic Access
Organization:	VISN 09 Memphis, TN
Date Opened:	1/6/2014
Date Closed:	1/21/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0600856
Date US-CERT Notified:	1/6/2014
US-CERT Case Number:	INC000000336930
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An anonymous phone call was received by the patient advocate that contends a CBOC Staff member at the Dyersburg CBOC is releasing private patient information. The phone number was on caller ID and the CBOC administrator and Assistant PO called the number and spoke with a Veteran . The Veteran stated he is going through a divorce and his soon to be ex-wife's aunt works at the CBOC. He is worried that this person can access his medical record.

Incident Update

1/10/14:
The veteran's record was marked as sensitive. Initial fact finding has found that no patient information has been released.

Resolution

No violation was found. The anonymous caller made accusation the Veteran did not confirm . The Veteran's record has been marked "Sensitive". Any further incident would be identified.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000099129
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	1/15/2014
Date Closed:	2/3/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0601187
Date US-CERT Notified:	1/15/2014
US-CERT Case Number:	INC000000338948
Category:	Category 4- Improper Usage
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Collection of individually Identifiable Health Information from the Veteran health record without a waiver of HIPAA or a signed authorization stating that this information will be collected. The incident involves a research study entitled “A Prospective Evaluation of PTSD Symptoms Following CPAP Treatments for Sleep-Disordered Breathing in Veterans (IRB #328000)” that was closed by the R&DC on September 2013 (Meghan McDevitt-Murphy, PhD.) for which neither the approved Waiver of HIPAA or the signed HIPAA authorization approved the collection of the Veterans ' SSN and phone number. In this case, the study team collected this information for 480 Veterans.

Incident Update

01/22/14:
The information did not leave VA control, this was discovered during an audit by the research compliance officer of the data requested . The Investigation Review Board will meet and discuss the course of action.

Resolution
No breach.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000099474
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	1/22/2014
Date Closed:	2/5/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0601500
Date US-CERT Notified:	1/22/2014
US-CERT Case Number:	INC000000340565
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

A Veteran complained to Memphis VAMC Customer Service Office regarding a travel voucher he received in the mail . He stated that in the window of the envelope (mailing label) anybody could see his full name, address, date of birth, and full social security number. He stated that he has already had trouble with identify theft in the past and this was just an open door for another identity theft. The Veteran did not understand why all these pieces of information should be displayed in the window of the envelope and therefore requested an investigation into the VAMC mailing process .

Incident Update

01/24/14:
PO received feedback about fact-finding conducted by the Supervisor assigned to Eligibility Department. She indicated one of her staff mailed the travel voucher to the Veteran in window envelope which exposed the patient identifiable information as stated in the complaint . Based on the fact-finding feedback, PO is of the opinion that the complainant PII may have been inappropriately exposed during the mailing process and should be given credit monitoring with promotion code.

The Veteran will receive a letter offering credit protection services .

Resolution
During fact-finding process, the Supervisor over the Eligibility Department agreed to provide education to staff and also stop using window envelope to mail travel vouchers. PO will follow during Privacy Rounds to ensure that staffs adhere to guidance provided by their Supervisor to avoid future occurrence of this type of incident. Based on the nature of the incident, PO determined that the Veteran's SSN may have appropriately exposed. PO has mailed Credit Monitoring letter to the affected patient, and also uploaded a Redacted copy to the case file in PSETS.

This incident is considered closed as of 2/5/2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000099694
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	1/27/2014
Date Closed:	2/12/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0601688
Date US-CERT Notified:	1/27/2014
US-CERT Case Number:	INC000000341708
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

A caregiver of a VA patient reported to the Privacy Officer that her client received an outpatient pharmacy co-pay exempt letter in the mail from Memphis VAMC. She stated the letter displayed the patient full SSN together with other information such as mailing address in the window of the envelope. She explained further that the way the letter was prepared and mailed makes it easy for anybody to see his client full name, address and full social security number.

Incident Update

01/27/14:
Veteran A will be sent a letter offering credit protection services.

Resolution

PO met with the Supervisor and Chief of Business Office to resolve the incident. As a short term safeguard, and beginning immediately, the Medical Support Assistants will mail correspondence with sensitive personal information in "windowless envelope" to prevent inappropriate disclosure of Veterans personally identifiable information as it did happen in this case. For a long term safeguard, PO will work with OI& T to remove SSN from all patient correspondence template.

Credit Monitoring letter has been signed by the Medical Center Director and will be mailed tomorrow. Incident is considered closed as of 2- 11-2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000099801
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	1/28/2014
Date Closed:	2/21/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Memphis Research Compliance Officer (RCO) performed an audit of an active research study and found that HIPAA authorization for the study does indicate the following identifiers will be collected about the enrolled research subject's: name, SSN, email and mailing address and phone number. Upon further review, the RCO identified that there were no waivers approved to enable the research investigator to collect this information. There are currently 140 subjects enrolled in this study which is in data analysis stage. Study was originally initiated on 2/9/2011.

Resolution

Investigator through her response to PO fact-finding admitted she and her research team were responsible for the lapses which resulted in the collection of identifiable information which were not noted on the HIPAA Authorization form. She stated she and the research team had very little knowledge that these identifiable information needed to to clearly provided on the HIPAA Authorization form. She stated however that the data (paper records) was collected and locked in a file cabinent in her research office and electronic data resided on VA network on P-drive. PO educated her about preparation of HIPAA Authorization and its legal importance. Based on the information provided by the Investigator, PO determined no PII was compromised as a result of this complaint. Complaint is considere colosed as of 2-21-2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number: PSETS0000100042

Incident Type: Mishandled/ Misused Physical or Verbal Information

Organization: VISN 09
Memphis, TN

Date Opened: 2/3/2014

Date Closed: 2/19/2014

Date of Initial DBCT Review: N/A

VA-NSOC Incident Number:

Date US-CERT Notified: N/A

US-CERT Case Number: N/A

Category:

Date OIG Notified: N/A

Reported to OIG: N/A

OIG Case Number: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

A Veteran reported to a telephone care staff stating he received medication for another veteran who gets her care at the Memphis VAMC . His explanation was that when he opened his medication package, he found it contained medication for another Veteran – i.e. mailed in the same package. Upon further review, the telephone care staff identified the medication was mailed out to the complainant from Memphis VAMC SCI Pharmacy .

Resolution

Through the fact-finding, it was determined that SCI Outpatient Pharmacy was responsible for mailing out the medication to the wrong patient. PO spoke with the patient who received the med; he confirmed that the medication came in an envelope with his address on it. He also stated the only identifiable informaiton on the med was patient full name.

PO has followed up with the Chief of Pharmacy and assigned supervisor(s) at the SCI Outpatient Pharmacy to provide education to the staff to avoid future missmailing of medication. PO determined that no PHI was compromised due to missmailing of the medication. Complaint is considered closed of 2/19/2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000100118
Incident Type:	Unauthorized Electronic Access
Organization:	VISN 09 Memphis, TN
Date Opened:	2/4/2014
Date Closed:	2/5/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0602087
Date US-CERT Notified:	2/4/2014
US-CERT Case Number:	INC000000344036
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

On February 3, 2014 at approximately 1:30 PM an employee reported to VA Police that someone hacked into his computer while he was logged on and that certain email was removed.

Incident Update

02/04/14:
Upon arrival at the complainant location, I met with VA employee (complainant). The complainant stated the he was log onto VA computer (MEM-WS 60447) and while viewing his VA email and yahoo email, he notice a box in the right hand computer pop-up and that seconds later he did not have control of his mouse. The complainant stated the someone was moving the mouse around without his control and he attempted control but was unsuccessful, so he quickly hit control, alt, delete, to close the program. The complainant also stated then he logged off. The complainant further states that he logged back into his workstation and that he did not see the pop-up box anymore and he was able to used his computer. As he went back to his email hours later, the complainant states that he notice the emails he was viewing earlier before the incident, was no longer there and that person who remoted into his computer had deleted his emails.

My investigation reveals that a OI&T service ticket was entered by another VA employee who's located in the same office as the complainant. The VA employee (non-complainant) entered the OI&T service ticket because the VA computer (MEM-WS60047) did not have any scanner software on it.

Further investigation also reveals that on February 3, 2014, @ approximately 0735, OI&T personnel contacted the VA employee (non-complainant) to see if anyone is log onto VA computer (MEM-WS60447). OI&T personnel stated he did not get an answer and the he left a voice mail. OI&T personnel further stated that he went ahead and log into the above VA computer to attempt to load software, but he notice someone was log onto the computer so he disconnect the connection.

Investigations also reveals that the VA employee (complainant) deleted some old emails prior to the incident took place, but wasn't sure if the emails that he was reviewing was deleted by him or OI&T personnel.

The complainant will be double checking his deleted, inbox and send boxes to see if the emails in questions are still located in his VA outlook email and he will notify the ISO office of his findings.

Investigation is outgoing pending the complainant findings of his email search.

02/05/14:
OI&T had remoted into the computer. no data breach occurred.
The complainant inadvertently deleted emails in questions, but stated he have them saved....

Resolution
Recommended to Memphis VAMC FCIO to create a SOP on servicing employees workstation via remote access (Dameware)

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000100163
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	2/5/2014
Date Closed:	2/11/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

During the Research Compliance Officer (RCO) audit of a research study entitled “VALOR-II: Randomized Controlled Trial of CBT for Co-Occurring PTSD and Alcohol Abuse”; study number 327996 (MIRB #00736), the he noted that the HIPAA authorization used to enroll subjects for this study did not list all the information that would be collected. Specifically, the authorization does not list the collection of name, SSN, mailing and email addresses, voice recordings and phone numbers. The HIPAA authorization does not specifically indicate what 38 USC 7332 protected information will be collected or how it will be used, but Investigator’s Checklist does state that information and treatment records related to alcohol and substance abuse will be collected for the study . Study was approved by IRB in 8/10/2011. RCO noted that 15 subjects were enrolled.

Resolution

During a review of the incident, PO and RCO determined that the incident occurred due mainly to minor issues IRB and PO overlooked during review and approval stage of the protocol. On PO's part, he should have reviewed the Research Checklist alongside with HIPAA Authorization to ensure the Investigator's statement regarding access and use of identifiers was consistent in both documents. PO may have overlooked the checklist and then reviewed/approved only the protocol and HIPAA Authorization. Similarly, IRB, in reviewing to approve the protocol did not verify the consistency between the Research Checklist HIPAA Authorization. The incident has been thoroughly discussed by PO and Assistant PO who have taken the lesson learned from the audit to improve their future reviews of research protocols to avoid a repeat of such an incident. RCO will discuss the incident and resolution during the upcoming IRB meeting. PO will be attendance of the meeting. It was determined that no PII was compromised since the investigator kept the data in her locked office and in a locked cabined .

Complaint is considered closed as of 2/11/2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000100312
Incident Type:	Missing/Stolen Equipment
Organization:	VISN 09 Memphis, TN
Date Opened:	2/10/2014
Date Closed:	2/24/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0602279
Date US-CERT Notified:	2/10/2014
US-CERT Case Number:	INC000000346573
Category:	Category 1 - Unauthorized Access
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

According to the Memphis Logistics Equipment Technician and the Chief Information Officer (CIO), the turn over inventory has been completed and the facility has one encrypted laptop and 14 desktop PCs missing. OIT is conducting a search of paper turn in records to attempt to locate evidence of the devices being turned in.

Incident Update

02/10/13:
Per the Memphis CIO, the laptop has been found. OIT is continuing the search for the 14 desktop computers. They are searching for them in the turn in paper work also. In addition, the facility CIO has asked VISN Logistics to assist them in searching for these items.

02/13/14:
According to the Information Security Officer (ISO), an update has been requested. The ISO is awaiting the response from the CIO.

02/19/14:
Per the CIO, there was 1 laptop and 13 desktop PCs missing, for a total of 14 devices missing. The laptop and 9 PCs were located. OIT believes the remaining 4 PCs were turned in and the hard disk drives disposed of. Because these are so old, there are no records that can tie the serial numbers of the drives to the Equipment Inventory List (EIL) numbers. Since the devices were so old, it is doubtful they were encrypted.

Over the years employees have always been educated/advised never to save sensitive information on the hard drive. The Inventory Tracking (EE) numbers and hard drive serial numbers are now recorded on VA form 0751.

Resolution
Inventory is conducted once per year. If the actuary rate falls below 95%, it is conducted twice per year. Logistics generates the EE number or barcode number. The Inventory Tracking (EE) numbers and hard drive serial numbers are now recorded on VA form 0751.

The IT Custodial Officer is responsible for ensuring that each hard drive is marked with the EE number of the host system whenever the hard drive is removed from the
host system. The EE number shall be written on the hard drive with an indelible marker at the time the hard drive is removed from the host system. ISO has verified with OIT Hardware Team Lead that this process is being followed.

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 not included in this report, but are included in the " IT Equipment Inventory Incidents" count at the end of this report.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000100602
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	2/18/2014
Date Closed:	3/4/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0602553
Date US-CERT Notified:	2/18/2014
US-CERT Case Number:	INC000000347254
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

A Veteran arrives in the outpatient lab without an appointment and produced an appointment letter intended for another Veteran . It also contained medication refills and clinic appointments. No SSN was present.

Incident Update

02/18/14:
IRT update: Veteran B will be sent a notification letter.

Resolution

This incident has been investigated with the staff from Pathology and Laboratory Department and the other Veteran involved . During the fact-finding process, we determined the paper was left on the printer in error and remained unattended until the other Veteran found it . This was confirmed by both Veterans during telephone conversations with the Privacy Officer on February 26, 2014. Please be advised that the paper was recovered from the other Veteran and shredded immediately after he reported the incident. In order to prevent future occurrence of this incident, the facility Privacy Officer will reinforce patient education within the waiting and check-in areas through privacy related posters and flyers. No Personally Identifiable information was ever compromised other than full name.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000100766
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	2/21/2014
Date Closed:	3/6/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

During an audit performed by the Memphis VAMC Research Compliance Officer (RCO) on a research study entitled “Ambulatory Care Assessment and Feedback for OEF/OIF Veterans (STRIVE)”, he found that the Investigator had inappropriately collected mailing and email address, phone number(s), DOB and information related to hospitalizations, disability rating (percentage) and OEF/OIF deployment information for approximately 955 veterans that was not covered by the signed HIPAA authorization or an approved HIPAA waiver. The auditor noted the Investigator obtained recordings of counseling sessions involving study subjects without acquiring a signed VA Form 10-3203 and also VA Form 10-5345 which authorizes the voiced recording to be released outside research environment. It was noted the Investigator later transferred the voice recordings of the counseling sessions to the University of Memphis for review. The voice recordings were for approximately 39 veterans enrolled in the study. Records available indicate the voice recordings have since been destroyed/removed from the University of Memphis server. RCO determined that the research study initially began in 2007 and it is currently open only for data analysis.

Resolution

During PO's fact-finding, the Research Investigator admitted the error and research non-compliance regarding this incident. She however attributed what occurred to "combined" Informed Consent and HIPAA Authorization document which was used in those days when she initiated this study . She said it was very confusing and all the research team could determine what the requirements were. She stated the combined document did not state clearly the type of protected information including PII that needed to be stated on the forms by the Investigator. She however agreed that now that Informed Consent Document and HIPAA Authorization are two separate documents, she understands clearly the requirements on both documents especially the HIPAA Authorization .

Regarding the Voice recordings of the therapy sessions , she admitted that part of it was sent to be kept temporary on University of Memphis secure Server located at her Research Lab. According to her, she transferred all of them from the secure server to the VAMC Network drive where they have been securely kept up to date. PO has verified the location of the Voice recordings of the therapy sessions on Memphis VAMC network drive . In all there about 41 recorded therapy sessions which are assigned random numbers as key by the Principal Investigator.

When asked as to what happened to the Voice records left on the University of Memphis secure server , she responded that they were destroyed after she transferred all of them to Memphis VAMC P-drive.

Regarding the state of the data including PII that was corrected, she stated she kept all of them in a locked file cabinet in his VAMC Research Office and never transported them outside the Medical Center.

PO provided guidance advising that since she (Principal Investigator) has been involved in series of research non-compliance issues, she should pay attention to earlier educational guidance provided regarding PII and PHI disclosure statements Investigator is supposed to make on HIPAA Authorization or HIPAA Waiver .

PO determined that since the data collected was secured in Investigator’s Office at the Memphis VAMC and the Voice recordings contained therapy sessions issues, there could not have been PII compromise resulting from the incident. PO considers this case closed as of 3/6/2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000100768
Incident Type:	Missing/Stolen Equipment
Organization:	VISN 09 Memphis, TN
Date Opened:	2/21/2014
Date Closed:	2/24/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0602726
Date US-CERT Notified:	2/21/2014
US-CERT Case Number:	INC000000348009
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

At approximately 0810, The ISO office received an email from Memphis VAMC Bio-Med supervisor in reference to the theft of EKG machine SD card. Equipment Info: Name: MAC 5500 EKG Cart, Model: GE MAC 5500 HD, EE#: 61117, Located in room #: 6170G of the Memphis VAMC Triage area.

The Bio-Med supervisor statement as follows: Yesterday morning around 8:30AM, one of my staff members received a call about an EKG cart in triage not saving EKGs. When he looked at the cart to troubleshoot it, he noticed the SD card in the back of the machine was missing. This is the temporary storage for the EKGs until it is plugged into a network port to upload the EKGs. However, the EKGs on the card can only be read via special software, so the information cannot be pulled for someone to read it outside of the hospital. The Bio-Med supervisor continue to state in the email that she spoke to the staff in this area , and no one knew where it was, so she would just caution that when you are not using the cart to please store it in a place where it is not easily accessible to patients and visitors. We are contacting GE this morning to see if there is a better way to lock this down , but I do not believe there is as you have to be able to remove this in case there is an error

Incident Update

02/21/14:
There is personal information stored on the SD card and the staff do not track how many EKG 's are taken so there is no way to know how many patients may have information ont he card. The information stored, however,requires the MUSE sustem to be able to read it.

Resolution
Staff have been informed that when a EKG cart is not being used, place the cart back in the secured triage room.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000100797
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	2/21/2014
Date Closed:	3/10/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An inidividual who is an employee and also a Veteran reported that 23 VAMC staff have accessed his medical record without proper authority , and that this ia violation of his privacy.

Resolution

PO has received responses from some employees (who are part of 23 VAMC staff) alleged to have accessed complainant record without permission or need-to-know. When PO tried to speak with complainant to ask him to assist in reviewing his medical record to provide any hint for one of of the accused employees to validate his access, he (complainant) stated to PO that "I'm not going to talk to you again on this matter" and then hanged up the phone. There are few responses PO has received which require further communication with complainant, but since he is not willing to speak with PO about matters arising from the fact-finding process PO is trapped and cannot proceed with the entire process. Theefore PO is requesing that complaint be closed due to complainant lack of cooperation to investigate the allegation. At 3:40 pm, complainant sent RMS "restricted" email to intimate the PO.

Complaint is considered closed; complainant will be notifed about the outcome of the fact-finding of the allegation.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000100911
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	2/25/2014
Date Closed:	3/18/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A VA employee reported to PO that his immediate supervisor stood behind him without prior notice to read his email while he was typing.

Resolution

During the fact-finding the Supervisor provided statements to validate that it is his supervisory responsibility to walk around in the work area to acquaint himself with the work being performed by his staff. He admitted that he routinely moves around in the work area without providing notice of his presence. PO and Assistant PO interviewed two of the employees about the Supervisor moving around to inspect work being done. They both admitted that they don't see anything wrong with the Supervisor moving around in the work area to acquaint himself with the work being done. They admitted that the assigned task is official VA job which they are required to accomplish.

PO and Assistant PO did a visual scanning of the work area and determined that the environment does not guarantee personal privacy for employees and that the complainant should be aware of this situation. PO noted that if employees engage in personal activities within such an environment, they risk having their privacy violated which the agency will not be liable. Therefore, PO found this complaint invalid and closed as of 3/18/2014. Complainant will be notified about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000101192
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	3/4/2014
Date Closed:	4/9/2014
Date of Initial DBCT Review:	3/11/2014
VA-NSOC Incident Number:	VANSOC0603124
Date US-CERT Notified:	3/4/2014
US-CERT Case Number:	INC000000350821
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

On Wednesday, 02/26/14, a Biomedical Engineer was told by an RN that the loaner Volcano Intravascular Ultrasound (IVUS) unit needed to be inspected so it could be used for an endovascular aneurysm repair (EVAR) case Monday, 03/03/14. The Biomedical Engineer told the RN that he needed the current preventive maintenance documentation. Also, he needed to fill out the loaner documentation. The Biomedical Engineer told the RN to contact former implant coordinator, on how to complete the loaner documentation for surgery.

On Thursday, 02/27/14, since the Biomedical Engineer had not received the preventive maintenance documentation, he called the sales representative, and left a message on her voice mail. When he checked his e-mail, on Friday, 02/28/14, the preventive maintenance documentation had been e-mailed to him. The loaner Volcano IVUS unit preventive maintenance was up to date (PM performed on 08/28/13. Next PM due August 2014.) The Biomedical Engineer performed the electrical safety inspection on the unit. While checking the unit he discovered that there was patient's information left on the unit from past cases. The information included names, social security numbers, and birthdays. He notified the Acting Biomedical Engineering supervisor, the RN and Surgical Manager. Since the patient was already scheduled for the case on Monday, Biomed Engineer recommended to Acting Biomedical Engineering supervisor and Surgical Manager that the unit should be used, but the loaner unit should not leave the hospital until it was determined how to remove the patient's information. Surgical Manager locked the unit in his office. Biomed Engineer still reminded RN and Surgical Manager that the loaner documentation needed to be completed.

On Monday, 03/03/14, when the Biomedical Engineer arrived to the hospital at 9:00 AM, he went to surgery to check on the status of the unit. The unit was being used on the first case scheduled for room one. He told the charge nurse that he needed the Volcano unit when the case was completed. She notified him and he went and took the unit to the Biomedical Engineering shop. He checked the unit and found that the past patients' data was missing. The only patient data remaining was from the case performed that day. He called the sales representative, and she told him that she deleted the patients from the database. Also, she went to the Windows operating system level and deleted the patients' folders. He told her that he has the unit and asked her what it would cost to replace the hard drive? He received a quote from Volcano and the cost to replace the hard drive is approximately $4762. As far as he knows surgery did not complete the loaner documentation, but the RN or Surgical Manager can confirm that. The Biomedical Engineer asked the sales representative who ordered the Volcano unit and she said it was the resident physician. Since Chief Biomedical Engineering was not here on Friday, the Biomedical Engineer informed her about situation on Monday, 03/03/14.

The equipment is secured in the Biomedical Shop. The Information Security Officer (ISO) and Biomedical Engineer are attempting to find resolution for removing data from hard-drive via VA approved method or retaining the hard-drive.

Incident Update

03/10/14:
The loaner unit was originally removed from the hospital by the sales representative in September of 2013. The loaner unit was stored in the sales representative's garage from late September until it was brought back to the VA as a loaner unit again. According to the sales representative, the device was locked in her garage during the time it was in her possession. The unit was off site from September 2013 until February 2014. The facility has received a statement from the sales representative indicating that fact. The number of patients whose information was on the device is between 1 and 10. Information at risk includes: Full name, partial SSN and DoB.

When the sales representative brought the unit back, she deleted the older patient information, both from the Volcano IVUS database and then deleted the folders from the Windows OS level.

Device security information: There is no log on to the device and no log on to the application software. The hard drive is not encrypted (medical device). The data is stored in a Volcano proprietary format.

03/25/14: The DBCT determined that this is unauthorized disclosure is of low risk of compromise.

Resolution

The hard-drive will not be returned to vendor, it will remain with Biomed and be processed for media destruction. Biomed will contact Surgical Service regarding payment for the drive. Meeting to be convened with Surgical Service, Biomed, Logistics, Privacy Officer (PO) and ISO to bring awareness of proper procedure and paperwork for using loaned equipment and the importance and means of protecting VA sensitive information . VA sensitive information is not to be entered on loaned equipment, a unique identifier should be used instead.

Remediation will also include Surgical Staff members review of MCM 00-82, Vendor Visitors on VA Premises. This facility policy specifically outlines procedures to be taken prior to a vendor coming to the facility, into a clinical area, that also involves outside equipment.

A multi-disciplinary team comprising Associate Medical Center Director, Assistant Medical Center Director, Associate Chief of Patient Care Services, Chief of Staff, PO, ISO Biomedical Chief, Chief of Logistics, Engineering, and 3 providers from Operating Room met. Logistics will provide training to Surgical Service staff of documentation to be completed when loaner equipment is needed. Surgical Service will create Standard Operating Procedure (SOP) to outline process for staff to follow. Service will come up with unique identifier for identifying patient on the equipment.

03/11/14:
The Data Breach Core Team (DBCT) requeststhe Incident Resolution (IRT) staff to find out if there was a VISN or local Business Associate Agreement (BAA)

03/18/14:
IRT reports back that there is no VISN or local BAA. DBCT requests to find out if the acquisition of the loaner device is accomplished via contract or purchase order.

03/25/14: The DBCT determined that this is unauthorized disclosure is of low risk of compromise.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000101260
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	3/5/2014
Date Closed:	3/17/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An employee reported to PO that his subordinate staff has obtained information pertaining to his federal student loan which was indicated on his application form for federal employment submitted to the Memphis VAMC. He clarified that when he applied for his current position from his former job, the application form required him to disclose informaiton pertaining to his student loan. He stated that he was successful with the interview process and was selected for the job. According to complainant, his subordinate has indicated to him that she has knowledge of his student loan infomation (amounts). Complainant believes someone who has access to his personnel folder has obtained this sensitive informaton and is sharing it with his co-workers.

Resolution

After carefully reviewing the responses provided by the primary witness to the complaint, PO determined that there is no evidence to prove that complainant personal privacy was violated. Complaint is therefore considered closed as of 3/17/2014. PO will notify complainant about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000101372
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	3/7/2014
Date Closed:	3/10/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0603289
Date US-CERT Notified:	3/7/2014
US-CERT Case Number:	INC000000352076
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Biomed employee was troubleshooting two VLANS with GE and Varian to try to get them to be able to communicate. He took a screen shot to try to show them what was happening with the work list. He did not notice that there was patient information on the screen shot, and he sent the email unencrypted to 2 vendors, Regional OIT, and the Information Security Officer (ISO). Once he realized it had patient information, he immediately recalled the message, which was successful for several people, but not all. He also instructed the vendors to delete the email with the information. The ISO has checked the Business Associate Agreements for both vendors, and both are active and they are allowed to view patient information. The employee explained this to the ISO today, and the ISO reminded him that he needs to be very careful and encrypt any emails that contain patient information. He said that he understood, and this was just an accident but that he would be very careful in the future. The ISO believes that all necessary actions were taken to remedy this situation.

One patient was involved with first and last name and full SSN.

Remediation: The message was recalled, and the vendors were asked to delete the email. We have one confirmation from GE that the email was deleted. We still have not received confirmation from Varian that the email was deleted. Both vendors have Business Associate agreements that are active and therefore they are allowed to view this information. The only issue was the fact that it was not encrypted when sent. Biomed Supervisor has spoken with her employee about this, and he understands that he has to encrypt emails. This was just an accident in this case. Employee has been education again how to encrypt email.

Incident Update

03/10/14:
The Incident Resolution Team has determined that no data breach has occurred. The document was seen only by VA trusted agents.

Resolution
Remediation: The message was recalled, and the vendors were asked to delete the email. We have one confirmation from GE that the email was deleted. We still have not received confirmation from Varian that the email was deleted. Both vendors have Business Associate agreements that are active and therefore they are allowed to view this information. The only issue was the fact that it was not encrypted when sent. Biomed Supervisor has spoken with her employee about this, and he understands that he has to encrypt emails. This was just an accident in this case. Employee has been education again how to encrypt email.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000101375
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	3/7/2014
Date Closed:	3/18/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Veteran reported that he enrolled in the Memphis VAMC PTSD Residential program and graduated on February 7, 2014. He stated that the program required participants to share their individual trauma experiences during group sessions. According to him he had Military Sexual Trauma (MST) experience while in the Service and this has impacted him emotionally and socially. He felt there was a need to share his bitter experiances with the group. Later on one of the participants in the PTSD group discussed his experience outside the group with another Veteran who in turn disclosed it to complainant 's friend who was enrolled in the Medical Center CDC program. Complainant's friend called and notified him about this inappropriate disclosure.

Resolution

In order to prevent future occurrence of this incident in the PTSD Residential Program, the Program Coordinator agreed to review and modified the Resident Manual (handbook), section 20 which deals with Veterans Privacy/Confidentiality. PO noted that this section does not provide privacy expectations which participants need to be aware of. Therefore, PO requested this section to be expanded to make privacy expectations more clear and understandable to all participants. The program Coordinator has provided a copy of the Resident Manual (handbook) to PO to review. PO concurs with the requested revision. Therefore complaint is considered closed as of 3/18/2014; complainant will be notified about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000101541
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	3/13/2014
Date Closed:	4/1/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

During an audit performed by Memphis VAMC RCO on a research study entitled “Multi-Site Evaluation of Progressive Tinnitus Management”; study number 312087 (MIRB #00698). He (RCO) found that the approved HIPAA authorization did not authorize the collection of study subjects’ names , mailing addresses and phone numbers. In addition, it was found that video/voice recordings of study subjects were transferred to the Portland VAMC without signed VA Form 10-5345. The RCO also noted that VA to VA Data Transfer Agreement was not signed by the receiving institution. The audit could not determine how the recordings were transferred to the Portland VAMC which is the coordinating center for this multi-site research study.

Resolution

During PO's face-to-face fact-finding with investigator this afternoon, he expressed disappointment of his lack of understanding of HIPAA Authorization . He admitted that he is solely responsible for the error and non-compliance issues arising from the RCO audit. In his explanation, he stated that he misunderstood the term demographics and considered it to include full name, SSN, Date of Birth, race, gender, age, marital status, etc. His lack of understanding of elements of demographics misled him to fail to include appropriate language in the HIPAA Authorization to indicate SSN , mailing address, etc will be accessed and used during the research.

PO explained the terms demographics, PHI, and PII and provided examples of each to ensure the investigator will understand the need to account for each one of them when accessing and using them in a research study. Investigator expressed his understanding of PO's explanation of these terms and stated that he assumed incorrectly about matters regarding demographics and meaning of PII. He assured PO that he will use the experience gained in the fact-finding to prevent future occurrence of this incident. Complaint is considered closed as of 4-1-2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000101710
Incident Type:	Unauthorized Electronic Access
Organization:	VISN 09 Memphis, TN
Date Opened:	3/19/2014
Date Closed:	3/28/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An employee from Home Based Primary Care (HBPC) delivered an envelope and package to the complainant at the Union Ave location where he is currently detailed. When the envelope was handed to the complainant, the employee stated “you need more information on numbers 5 and 6 on your Family Medical and Leave Act (FMLA) paperwork.” The complainant's concern is there is no reason the other employee needs to know about FMLA claim . Secondly, when the complainant was in the HBPC office on 3/18/2014 the employee asked the complainant if he had received packages from nursing services. The complainant asked what packages? The employee stated that when they had returned from delivering the package the other day another employee said the complainant had three packages. The employee stated the packages were personal and that that the packages were part of the reasonable accommodation request. There is no reason this employee should know this information as they do not have a need to know about the complainant’s medical status or request for reasonable accommodation. There is also a concern that management is accessing the medical records

Resolution

In the course of the fact-finding, it has was been determined that the two secretaries identified by the complainant investigated for the incident performed in the scope of their official VA duties. Secretary one received the information from her immediate supervisor supervision and passed on to the complainant as directed. All packages were Package was sealed and she had no specific knowledge of what they contained. Secretary two received the information initially and opened for her supervision to ensure FMLA forms were properly filled out as required by her official VA duties to review . She performed her duties as required by her job specified by her supervision. A review of the complainants medical record revealed no unauthorized access by the individuals investigated for the complaint. Assistant PO determined that there was no evidence of a breach as alleged by complainant. Complaint is therefore closed as of 3/28/2014. Complainant will be notified regarding the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000101802
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	3/20/2014
Date Closed:	6/23/2014
Date of Initial DBCT Review:	3/25/2014
VA-NSOC Incident Number:	VANSOC0603692
Date US-CERT Notified:	3/20/2014
US-CERT Case Number:	INC000000355067
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

During the Research Control Officers (RCO) audit of the study entitled (Effect of DVT Prophylaxis Order Sets on Incidence of Venous Thromboembolism); study number 361723. The study was closed by the R&DC on August 14, 2013. The principal investigator (PI), is no longer affiliated with the Memphis VAMC. During the required RCO human research protections program (HRPP) audit of the study, it was found that the approved HIPAA waiver did not approve the collection of PHI related to admission, operation and discharge dates for the 583 subjects in this retrospective study.

Incident Update

04/01/14:
PO and Principle Investigator (PI) discussed the incident. The intent of this project was to evaluate the impact of a DVT prophylaxis order set on the incidence of DVT occurrence vs adverse events (i.e. bleeding). Since DVT prophylaxis is utilized while a patient is in the hospital & would prevent occurrence of DVT during or shortly after discharge the data query run for the study listed pulled DVT ICD 9 codes for thromboembolic events that were entered in close proximity to hospital stay. The data generated was reviewed for timing of event vs hospital stay for the pre and post DVT order set periods .

The HIPAA waiver did not include this information as it was not information that we planned to evaluate but was an unintended method of data collection used to decrease the number of unrelated cases of DVT reported in the data query . All of this data has been stored locally in a protected folder on the P:drive research folder and has not left the facility.

Resolution
The Investigator did not intent to access and use PHI which was not originally stated on his HIPAA Waiver form . According to the investigator, the query run for the study listed pulled Deep Vein Thrombosis (DVT) ICD9 codes for thromboembolic events that were entered in close proximity to the patient hospital stay. He stated the diagnosis pulled was unintended data extraction since it was not part of what the study meant to review.
The Investigator agreed that the HIPAA waiver did not include the PHI (i.e. diagnosis) as it was not information that he planned to evaluate but was an unintended method of data collection used to decrease the number of unrelated cases of DVT reported in the data query .
Regarding the protection of the data after it was extracted, he stated that all the data has been stored locally in a protected folder on the P:drive research folder and has not left the facility since it was extracted. Based on the responses provided by the Investigator, PO determined that there is no evidence to show that the PHI was viewed by other people, though the investigator's actions is non- compliance with VA research protocol procedures . PO determined that the research study in question is already closed and so there is no need to re-consent study subjects about the data that was unintentionally extracted.
PO discusses with the Investigator to ensure that in the future, he should test his data query methodology before applying it to his protocol to avoid extraction of data that is unrelated to the study.

03/25/14:
The study is closed. The facility is trying to determine the location of the Principle Investigator, who is no longer affiliated with VA. Also, the facility is investigating if the data is secured and the location where the data is kept.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000101922
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	3/25/2014
Date Closed:	4/1/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

The Memphis VAMC Research Compliance Officer (RCO), during his triennial Human Studies Research Protections auditing, identified that Research Investigator obtained information on VA patients for his study without seeking proper authorization for access and use of the data for VA research . The Investigator presented HIPAA Waiver to IRB but failed to disclose the relevant PHI/PII which would be accessed and used in the study. Review of the research records shows the Investigator collected different pieces of PHI and demographic information such as age , marital status, race, etc. Review of the study records also indicates the Investigator did not provide statements showing how the PHI would be safeguarded and protected in the course of the research. The RCO noted the Investigator did not present the protocol to PO and ISO for review before seeking IRB approval. It was also noted the study in question was closed by Research and Development Committee (R&D) on October 9, 2013.

Resolution

PO met with Investigator this afternoon to review the findings from RCO audit. Investigator admitted all issues identified in the audit findings and assured PO that he has learned his lessons from this event and will do everything possible to prevent future occurrence of this type of research non-compliance. PO reviewed all requirements of HIPAA Authorization and HIPAA Waiver with investigator. PO also drew Investigator's attention to all necessary safeguards that must be in place to protect PHI and PII collected and used in VA research. PO made him understand that failure to have safeguards in place to protect PHI/PII is considered a breach of inappropriate handling of VA Sensitive information. Also failure to disclose VA sensitive data to be accessed and used during research on HIPAA Authorization and/or HIPAA Waiver is a breach of VA access policy. Investigator expressed his understanding of everything discussed with him by PO during the meeting.

Incident is considered closed as of 4/1/2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000102612
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	4/9/2014
Date Closed:	5/12/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

The Chief of Radiology reported to the Privacy Officer (PO) that one of the Radiology Clerks accessed the department lockbox which contained Ultra-sound appointment requests sheets and then mis-handled the contents which resulted in 14 requests missing from the box. The Chief stated that the Radiology Clerk had no business needs reason to access the contents in the lockbox and wondered what she may have done to the missing requests on 14 patients who were scheduled for Ultra-sound appointments on April 5, 2014.

Resolution

After carefully reviewing the fact-finding statements presented by different employees, PO did not see any evidence showing the employee mishandled patient sensitive information and/or discarded it in inappropriate manner. Therefore PO determined there is no evidence of violation in any form. Complaint is closed as of today,
5-12-2014. The complainant, Service Chief, will be notified about the outcome of my fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000102657
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	4/9/2014
Date Closed:	4/10/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0604471
Date US-CERT Notified:	4/9/2014
US-CERT Case Number:	INC000000360621
Category:	Category 4- Improper Usage
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

VA employee SW sent unencrypted email containing the information below (1-3). Email was sent to internal VAMC MEM Outlook email address, (b)(6) which is an email address containing 52 persons.

1. Patient caregiver's first and last name; address. Entire HBPC team goes to the home to provide care for patient.
2. VA patient first and last name; last 4 SSN
3. VA patient last name; last 4 SSN

Incident Update

04/10/14:
An internal unencrypted email was sent to the intended recipients. The Incident Resolution Team determined that no data breach has occurred.

Resolution
ISO spoke with VA employee regarding importance of protecting PII and adhering to safeguards to protect data . Employee was instructed to check content of email for PII and ensuring she had selected to encrypt email before sending. The following remediation was done:

a. VA employee recalled and deleted email
b. VA employee tested encryption by sending ISO an encrypted email successfully
c. VA employee signed the ROB

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000102723
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	4/10/2014
Date Closed:	4/21/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Registered Nurse who is an employee at the Memphis VAMC came to the Privacy Officer's (PO) office in the company of AFGE Vice President and a Union Steward. She reported that her Supervisor has contacted her private Psychiatrist and requested information pertaining to her mental health evaluation/assessment. According the complainant, the Supervisor disclosed to the Psychiatrist that the employee has been showing erractic behavior which is a concern, therefore, getting a copy of her mental health evaluation will be helpful.

Resolution

PO has concluded his fact-finding on the incident. PO noted that though the Supervisor called and spoke with complainant's private psychiatrist, she did not release complainant's sensitive personal information of any kind. During the fact-finding, the Supervisor stated she only told the private psychiatrist “you wrote for employee ‘fit for duty note’ but her behavior at work is not appropriate." PO met with the witness identified by the Supervisor whose narrative statements confirmed what the supervisor stated. PO did not see any evidence of HIPAA violation because the statement made by the supervisor does not constitute a disclosure per se. The fact of the matter is that she (supervisor) did not release any specific PHI or medical condition. PO however re-educated the supervisor on the cause of action she took which made her narrowly escaped HIPAA violation. PO made her aware that a Supervisor cannot call to speak with employee’s private provider about matters pertaining to the employee without seeking an authorization/permission. Complaint is considered closed as of 4/21/2014, PO will notify complainant about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103046
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	4/18/2014
Date Closed:	5/23/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Wife of a Veteran sent a video clip of her husband, another Veteran and a VA Physician to Memphis VAMC Patient Advocate . The wife complaints that the provider was discussing sensitive information pertaining to both Veterans in the same room with the Veterans listening to each other 's medical and sensitive private issues at the same time. The wife reported that this is a violation of HIPAA privacy rule. The wife contended that it is inappropriate and unethical for diagnosis of each patient to be discussed in the presence of both patients. She stated her husband was at the hospital for a GI procedure.

Resolution

The follow up and fact-finding indicated the provider who was video-taped by the patient wife was performing his official VA duties as outlined in the GI Clinic policy. Due to lack of staffing, it became a policy for GI Clinic to consent more than one patient in a room to enable staff to handle daily workload without having a backlog. In this kind of situation, two or more patients with their family members would be in the same room to be consented by a physician for their upcoming procedure.

In order to remediate this incident, it has been documented that all patients in the GI Lab will obtain their written consents individually in an empty room. Only the individual patient or patient's family members will be present in the room when the physician obtains the consent in the GI Intake rooms . Nurses may be present within the Intake room during the consent process, but no other patients or patients' family members will be allowed in the room. This will be part of the GI new policy and all staff will be educated about it.

Complaint is considered closed; Patient and/or his wife will be notified about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103116
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	4/21/2014
Date Closed:	5/23/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A patient admitted to the SARRTP program stated that former patient in the program, who was discharged on 4/17/2014, told him (complainant) he had learned about an incident involving him (complainant) that occurred in the past (January 2013) from one of the nurses for the SARRTP program. According to the complainant account, the nurse talked to his informant and shared with him the story about how she (the nurse) had intervened on complainant's behalf while he (complainant) was using drugs on the unit during his previous admission. Complainant stated he was admitted to the SARRTP Unit January 16-22, 2013. The nurse disclosed to the informant that complainant's syringes were discovered in the trash can in his bedroom and close to the urine sample (provided by another patient) which complainant attempted to pass off as his own urine. Complainant stated the story was true, and he believed that the nurse had told his informant everything about it. Complainant is upset that SARRTP nurse has violated his privacy because found out that his informant disclosed this same information to another patient who was at the smoking shelter.

Resolution

Upon review of the summary fact-finidng report submitted by the Nurse Manager, PO determined that there is no evidence of a privacy violation. Later on during the investigation, complainant (a patient) approached the nurse being investigated and looked very remoserful stating he was having some “doubt” about the incident and was not certain that the incident occurred exactly as he initially believed and reported. His demeanor shows the complaint was invalid and that he was not pressing charges against the nurse.

Complained is considered closed, PO will notify complainant about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103203
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	4/23/2014
Date Closed:	5/6/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

During an audit performed by the Memphis VAMC Research Compliance Officer (RCO), he found a VA research investigator had accessed and used study subjects name and SSN on a signed HIPAA authorization form which did not specify such information will be collected during the study . The RCO noted 89 subjects' name and SSN were collected in all. The audit finding also revealed that the Investigator collected protected information on13 study subjects who did not sign HIPAA Authorization at all.

Resolution

PO had a lengthy discussion with the Investigator regarding this research anomaly. PO noted from Investigator's responses to the fact-finding that Protocol is currently active.
Investigator admitted that the error is a non-compliance with VA Research policy and raises questions about subject's privacy and confidentiality. She also admitted the error was an oversight because she knew she would be using subjects name and SSN to review their records. Since the protocol is active, the Investigator stated, she is prepared to address all errors to allow her move on to complete the research study.
Investigator and RCO have reviewed protocol and they noted it is of minimal risk study which does not require HIPAA Authorization. It rather requires a HIPAA Waiver. The reasons are that:

1. The only PII that will be collected will be patient last name and last four of SSN.
2. That the outcome of the study and data to be collected will not be disclosed outside Memphis VAMC.

On the other hand, the investigator has been guided to revise the HIPAA Authorization to include the missing PII (ie. name and SSN). In the event IRB does not approve the protocol amendment to use HIPAA Waiver, then Investigator re-consent the subjects using the revised HIPAA Authorization.
Investigator stated that the survey data collected so far is being protected and resides in Investigator's protected folder on network drive. Regarding 13 subjects who completed the survey but did not show up to be re-consented their data will not be included or used for the study. If IRB approves the modified protocol, the other 89 subjects will be re-consented and their data will be used for this study.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103430
Incident Type:	Non-VA Responsible/Non-Incident Upon Further Investigation
Organization:	VISN 09 Memphis, TN
Date Opened:	4/28/2014
Date Closed:	5/14/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A VA employee, also spouse of a Veteran called to speak with a mental health provider about medications prescribed for her spouse . The statements made by the employee (spouse) about the prescribed medication made the provider suspect this employee and another staff from Memphis VAMC CBOC may have accessed and viewed the Veteran medical record without permission or a need-to-know. Meanwhile, PO has requested ISO to run a Sensitive Patient Access Report (SPAR) on the patient to determine if the two individuals have been accessing and viewing the patient medical record.

Resolution

During PO and ISO fact-finding conducted into the allegation, employee admitted accessing and viewing her husbands CPRS record multiple times. PO reviewed the SPAR report and noted that employee had accessed and viewed her spouse records about 14 times on different occasions. PO and ISO made it clear to employee that her behavior is a violation of VA policies. We explained to employee about VA access requirements and resultant consequences if employee violates the policy.

Complaint is considered closed as of 5/14/2014; employee supervisor has been notified about the outcome of the fact-finding conducted by PO and ISO into the complaint.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103432
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	4/28/2014
Date Closed:	5/12/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0605245
Date US-CERT Notified:	4/28/2014
US-CERT Case Number:	INC000000365775
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Eligibility staff mailed a travel pay request letter to a Veteran and accidentally included Travel Pay Request form pertaining to another Veteran . The information contained on the form accidentally mailed out are: full name and last four of SSN. The receiving Veteran called to notify the Privacy Officer at Mount Home VAMC who in turn reported the incident to Memphis VAMC Privacy Officer.

Incident Update

04/29/14:
The Incident Resolution Team has determined that Veteran B will be sent a general notification letter.

Resolution

Supervisor has met with employee to review work process and determined what may have let to the incident. Employee admitted she accidentally folded a Veteran's paper record and placed it into a correspondence envelope being mailed to another Veteran . During the meeting, supervisor emphasized on attention to detail and requested that employee should always check correspondence envelope twice to make sure contents of the envelope belong to the same and one person. PO determined that the PII contained on the document accidentally mailed out (travel request form) was Veteran full name and last four of SSN.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103630
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	5/2/2014
Date Closed:	5/2/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0605449
Date US-CERT Notified:	5/2/2014
US-CERT Case Number:	INC000000366485
Category:	Category 4- Improper Usage
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Business Office employee sent unencrypted email on 5/1/14 to an incorrect email group. According to employee, a supervisor in the Business Office gave her the email group name. After sending email, she received responses informing her that she sent to the wrong group and that it was unencrypted. The group she sent it to was VHA Mental Health Intensive Case Management. Employee's supervisor was asked to contact employee to find out intent and whom the message was supposed to be sent to.

Sensitive info included in the email:
3 patients: one with full name, last 4 of SSN and phone number
one with full name, last 4 of SSN and address
one with full name, last 4 of SSN, address and phone number

Incident was brought to the attention of the MEM ISOs by ISO at another VAMC, and she was informed by employee at her facility.

Incident Update

05/02/14:
The Incident Resolution Team has determined that an unencrypted e-mail was sent to recipients internal to the VA network. No data breach has occurred.

Resolution
1. MEM ISO met with employee and instructed her how to recall email; recall completed.
2. ISO gave instruction on how to send encrypted emails and when this must be done.
3. Employee sent 2 encrypted test emails to ISOs.
4. Employee has reviewed and signed the ROB.

ISO followed up with employee's supervisor regarding duties and whom the email should have been sent to. According to supv., employee normally does not send sensitive info via email but calls the eligibility section to provide updated info on patient or takes it to that section. The intended email should have gone to the eligibility group.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103654
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	5/2/2014
Date Closed:	5/23/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0605472
Date US-CERT Notified:	5/2/2014
US-CERT Case Number:	INC000000366571
Category:	Category 4- Improper Usage
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	7
No. of Loss Notifications:	

Incident Summary

The facility Blood Bank sent out patient blood samples with their sensitive personal information to a vendor in New York that has no formal business relationship or contract established with the VAMC. An employee from the Blood Bank reported the incident to the Information Security Officer (ISO) and Privacy Officer (PO) for follow up to determine if it was legally permissible to send out VA sensitive information to a company that has not formal business relationship with the VAMC. The PO has reviewed the incident and noted there are 7 Veterans who are affected by this incident: their full name, full SSN and date of birth were sent out together with the blood samples.

Incident Update

05/05/14:
The Incident Resolution Team has determined that seven Veterans will be sent letters offering credit protection services .

Resolution

CM Letters have been prepared for mailing. PO advised the Path and Lab Service not to send any more blood samples to outside lab service vendors that have no executed contract or Purchase Order prepared with ISO and PO signatures. PO has requested Path and Lab leadership to contact the company to make sure all paperwork they received with blood samples are shredded. To ensure that this incident does not happen again, the Chief of Path and Lab Service is requesting Blood Bank Supervisor to review all existing policies and procedures regarding "send-out samples" so his employees will be educated on existing requirements. Fact-finding is therefore concluded; PO is requesting that incident be closed.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103657
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	5/2/2014
Date Closed:	5/7/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A VAMC employee (a Registered Nurse) has noted that her husband's picture has been posted at various locations within the VAMC . She stated the bottom of the picture states that "Staff should call the VA Police when they see him enter the VAMC premises ." The complainant says, she has discussed the issue with her husband who is upset about his picture posted at various locations at the hospital. Complainant stated that posting her husband's picture in the manner she has seen it violates his personal privacy rights and demanded investigation into the matter.

Resolution

PO has concluded his fact-finding on the incident. Associate Chief of Staff for Patient Care Service was contacted who referred PO to contact VA Police for more information regarding the incident. VA Police indicated they were notified by Memphis VAMC Psychologist to act to protect the Veteran's wife and VA employees. The Psychologist provided Employee Assistance Counseling service to the complainant (wife of the Veteran). During the counseling session, the psychologist indicated the employee would be admitted to the Mental Health Ward (for 603). Employee then requested to speak with her husband to notify him about the impending admission. According to the report compiled by the VA Police, the Veteran was very violent on the telephone and threatened his wife (VA employee). The psychologist overhead the Veteran hurling abusive and threatening words at employee. The Psychologist also noted the demeanor of the employee (wife of the Veteran) changed abruptly so he felt there was need to notify the VA Police to act immediately to protect the employee and her co-workers.

VA Police therefore managed to obtain a photograph of the Veteran and printed copies for distribution at the Emergency Department and other locations so employees would be able to identify the Veteran and immediately notify VA Police in the event he shows up at the hospital.

Upon review of the incident, PO determined there is no evidence of violation resulting from the action taken by the Psychologist and the VA Police. Complaint is considered closed; complainant will be notified about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103857
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	5/8/2014
Date Closed:	6/2/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0605660
Date US-CERT Notified:	5/8/2014
US-CERT Case Number:	INC000000367715
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

A VA nurse received a call from a Veteran stating he received a letter in the mail from the VAMC on May 6, 2014 with another Veteran's appointment letter which shows his name, last 4 of his social security number, address and dates for all his scheduled clinic appointments. The Veteran stated his own correspondence was mailed along with the other Veteran's clinic appointment letter. The Veteran was concern about the other Veteran missing his scheduled clinic appointments. The nurse requested the Veteran to provide all PII that appeared on the letter including the Veteran first and last name. The nurse wrote the information down and requested Veteran to shred the letter which he agreed.

Incident Update

05/08/14:
The Incident Resolution Team has determined that Veteran A will be sent a notification letter.

Resolution
Notification letter is signed by the Directory and ready to be mailed. During the Business Office staff meeting, the Chief reminded all supervisors to re-educate their staff to ensure that they pay close attention to correspondence being mailed to Veterans. Supervisors were told to ensure attention to emphasize attention to detail especially among staff who prepare correspondence for mailing - checking each envelope twice to make sure all paperwork belongs to the same person. Complaint is considered closed.

Notification letter has been mailed to the affected Veteran.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000103861
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	5/8/2014
Date Closed:	5/30/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Veteran reported that a VAMC employee has accessed and retrieved her cell phone number from her VA records and used it to call her and also sent text messages. She stated that during her CT clinic appointment on 4/16/2014, the employee tried to exchange phone numbers with her however she did not like the idea of sharing her telephone number with him. According to her statement, the employee kept disturbing her and asked for her phone number several times. According to her statement, she reluctantly received the employee's telephone with the pretense that she would call to give hers to him . She believed this trick would make him stop harassing her with the request for her phone number. She stated she threw the employee's number away as soon as she left the hospital building because it was not her plan to communicate with him. According to her, on 4/24/2014, this individual called her to initiate a conversation but she declined to speak with him and asked "where did you get my number from?" The employee replied that she retrieved complainant's cell number from her VA records. According to complainant, the phone conversation ended right there, and then later on this individual sent text messages stating that he was concern about complainant's medical situation and was trying to call to find out how she was doing . Complainant believes this is a violation of her personal privacy because she never provided him any permission to access and retrieved her phone number. She also added that the purpose for employee retrieving her phone number from her VA records has nothing to do with his official VA duties .

Resolution

Po and the Supervisor over the CT scan area reviewed fact-finding statements made by both complainant and VA employee under investigation. Employee made inconsistent statements about how he obtained complainant's telephone number to initiate a phone call to her outside the VA. He stated complainant willingly provided her phone number during her CT scan visit. Complainant consistently denied this statement, and provided a copy of a text message she sent to him questioning about the means he obtained her phone number. When questioned why she (complainant) took employee phone number, she admitted employee was persistent in his request to get her phone number. In her own statement, she took employee phone number just to stop him from harassing her. She stated she never used the phone number to call him, because she did not have any reason to call him.

When complainant questioned employee during their phone conversation about how he obtained her phone number he (employee) replied he obtained the phone number from the CT scan paperwork complainant brought with her during clinic visit. PO verified if patient CT scan paperwork contain patient phone number. The Radiology Tech Supervisor clarified stating that CT scan paperwork does not show patient phone number.

PO determined that complainant medical record was not flagged as "sensitive record" so a SPAR report could not be run to determine whether or not the employee accessed complainant record at any time apart from the day complainant was seen at the CT scan area. Employee insisted that it was mutual agreement between the two of them to exchange phone numbers and that he was prepared to show his phone bill as evidence to support his statement that they both agreed to exchange phone numbers. However, employee supervisor made several appeals to get the phone bill but employee failed to provide it.

Upon carefully reviewing all the facts, PO determined that the employee accessed complainant record and impermissibly obtained her phone number for an activity that is not part of his official VA duties. Therefore, PO found evidence of violation regarding the complaint. Complainant will be notified about the outcome of the fact-finding; and employee supervisor will be notified with a copy of PO's summary report. Complaint is considered closed on 5/30/2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000104146
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	5/14/2014
Date Closed:	5/21/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Veteran reported to PO that he was intoxicated and needed assistance with the OEF /OIF social work staff. He stated further that he wanted to come in to the medical center so he could be detox. He stated that thought he provided his next-of- kin contact telephone to the social work staff, he did not specifically ask him to call to provide notification about his condition. According to the Veteran, the social work staff called and notified his mother (next-of-king) that he was intoxicated and needed assistance. Veteran stated this is a violation of his personal privacy because he did authorize the social work staff to provide such information to his mother.

Resolution

PO contacted the provider (OEF/OIF Social Worker) to get his full account of the incident. According to Social Worker, complainant called from home to request to be admitted to the hospital to be detox. Complainant was highly intoxicated and looked helpless. Staff noted he was home by himself and therefore needed assistance. Complainant provided his mother's telephone number to staff who called to alert her of the complainant's condition. Staff reviewed complainant's medical record and noted his mother is Next-of-King and that it was ok to release general information about the patient condition to her.

Upon review of the complaint, PO determined that the provider acted in the best interest of the patient; PO thus did not see any evidence of violation resulting from the action taken by the Social Worker. Complaint is considered closed as of 5/21/2014. Complainant will be notified about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000104270
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	5/16/2014
Date Closed:	6/23/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Employee reported a clinical disagreement with another clinical staff about a patient's clinical disposition to non -clinical entities (i.e. Local AFGE members) to voice her discord about impending clinical disposition of the patient. The message was sent via VA email system. It is unclear why the local AFGE members were notified about clinical matters and sensitive information pertaining to a VA patient which has not generated into Labor -Union issue. Complainant believes that this is not appropriate and that the local AFGE members in their capacity as Union staff do not have right to VA sensitive information unless they have requested for such information through the HR or FOIA officer.

Resolution

PO concluded his fact-finding on complaint on Friday, June 20, 2014 in the presence of the employee, her supervisor and two AFGE Union representatives. After PO provided background information regarding the complaint, the employee apologized for her action in the incident, and stated she was of the view that since the AFGE leadership are permanent VA employees, VA sensitive information can be shared with them when necessary, especially if they need it in the performance of their duties as Union leaders. PO used the fact-finding meeting as an opportunity to explain and educate employee about labor union role in the facility management and the authority union leaders use to get access to VA sensitive information if they have need for it . PO drew employee attention to two (2) statutes: Title 5 of USC, Section 7114(b) (4), this is union right to records in order to assist an employee during the disciplinary process. HR needs to make the determination as to what is required out of the evidence file for the union to have access to in order to represent and defend the alleged allegations. FOIA statute, Title 5 USC, section 552. This is a statute of disclosure which the Union can use to request additional information to defend employees if they are unsatisfied with information given them under 7114(b)(4) by HR. Employee verbalized her understanding of PO's education. Employee supervisor explained to PO that she met with employee prior to the fact-finding meeting and counseled her regarding inappropriate sharing of information with Union leaders. Supervisor provided a copy of her report of contact which highlights her discussions with employee when both met.

PO determined that no PII was compromised as a result of this complaint. Information shared was patient last name, last four of SSN, patient medical condition and his disposition.

Complaint is considered closed as of 6/23/2014. Complaint was brought PO's attention by another VA employee who received copy of the email employee sent to the AFGE leaders.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000104599
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	5/27/2014
Date Closed:	6/18/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0606363
Date US-CERT Notified:	5/27/2014
US-CERT Case Number:	INC000000371826
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Veteran suspects that he is a victim of a possible identity theft because he has never received medical care from Memphis VAMC but he keeps receiving patient care bills in his name. He stated that these bills have resulted in his income tax returns being garnished by IRS. He initially reported the incident to the Identity Theft Helpline and is requesting the Memphis VAMC to investigate this matter.

Incident Update

06/18/14:
PO requested incident to be closed due to the fact that complainant did not cooperate to provide necessary information regarding the bills he received from Memphis VAMC which he alleged resulted in the identity theft. PO called and spoke with him on several occasions but he failed to provide the requested information. Ticket may be reopened if more information is provided.

Resolution
As of today, June 10, 2014, complainant has not provided to PO the requested information needed to assist Memphis VAMC billing office to review his patient care services and all bills generated in his name. PO has spoken with complainant in person three times to request information needed for the review of his case but he failed to provide the requested information. PO also left call back messages asking complainant to call to provide the requested information but he failed to return PO's call.

PO has determined that the complaint is invalid because complainant is unwilling to assist the VAMC to review the case . PO is requesting that complaint be closed as of June 10, 2014. Complainant will be notified regarding the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000105098
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	6/6/2014
Date Closed:	6/13/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A VA research investigator accessed and used VA patient identifiable information in an approved research study with approved HIPAA Authorization but the identifiable information accessed was not specified on the HIPAA Authorization for review and approval before he accessed them . The personally identifiable information (PII) accessed is research subject's full name; SSN, address and telephone number.

Resolution

PO and Research Compliance Officer (RCO) have discussed this incident. This is a Corporative Study Program that is funded and controlled by VA Central Office. In all CSP research studies, the local PO does not review, approve or provide any guidance to local Research Investigators participating in the CSP studies. Thus, as a local PO, I do not have “jurisdiction” to investigate and resolve this issue at our local level here since the committee that is responsible for reviewing and approving CSP studies are not Memphis VAMC employees. RCO is supposed to notify Central IRB regarding this incident. Therefore the complaint is closed as of 6-13-2014 with no futher action required.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000105319
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	6/13/2014
Date Closed:	6/30/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0607064
Date US-CERT Notified:	6/13/2014
US-CERT Case Number:	INC000000376279
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Veteran reported that he received a package from the Memphis VAMC delivered to his home address by UPS and when he opened it , he noted it contained pharmacy medication prepared to be mailed to Veteran B. The medication wrapper had the full name and mailing address of the intended recipient (Veteran B).

Incident Update

06/13/14:
The Incident Resolution Service Team has determined that Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

Chief of Pharmacy Service has educated all staff assigned to prepare prescriptions for mail-out about safeguards they need to observe when preparing the medication to be mailed. Additionally, he has reviewed and revised the Standard Operating Procedure (SOP) used in the prescription mail-out section of the pharmacy. Copy of the SOP has been forwarded to the PO for review and his records.

Notification letter has been signed by Medical Center Director and it's ready to be mailed. Redacted copy of notification letter has been uploaded into PSETS, attached to this ticket. Complaint is considered closed as of 6/27/2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000105322
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	6/13/2014
Date Closed:	6/13/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Memphis VAMC Research Compliance Officer (RCO) audited a Corporative Study Protocol (CSP) research study, entitled:

A Randomized, Placebo-Controlled, Double-Blind Clinical Trial to Evaluate the Safety & Efficacy on Methylprednisone in Hospitalized Veterans with Severe Community-Acquired Pneumonia (CAP) – ESCAPe" CSP Study #574; study numbers 425796 (MIRB #00728) and (cIRB #10-04)

During auditing, the RCO noted that approved HIPAA Authorization (Version 9/30/2011) does not state that study subjects' name, SSN, address, dated of birth and phone number will be collected during the study. The information listed on the HIPAA form be collected does not include the above PII. The RCO noted this is in violation of VHA Handbook 1605.1, §14.b.(1)(b).

Resolution

PO and Research Compliance Officer (RCO) have discussed this incident. This is a Corporative Study Program that is funded and controlled by VA Central Office. In all CSP research studies, the local PO does not review, approve or provide any guidance to local Research Investigators participating in the CSP studies. Thus, as a local PO, I do not have “jurisdiction” to investigate and resolve this issue at our local level here since the committee that is responsible for reviewing and approving CSP studies are not Memphis VAMC employees. RCO is supposed to notify Central IRB regarding this incident. Therefore the complaint is closed as of 6-13-2014 with no futher action required.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000105769
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	VISN 09 Memphis, TN
Date Opened:	6/25/2014
Date Closed:	7/3/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

The Administrative Secretary within the Business Office received an unencrypted email from an employee from another Service . Complainant stated she has been receiving multiple unencrypted emails from this user which contained sensitive personal information.

Resolution

During PO's meeting with employee, she admitted sending multiples of unencrypted emails containing PII. She attributed the incident to her inability to effectively use PKI encryption in Microsoft Outlook. PO provided step by step education to walk employee through the encryption process. To ensure that employee was comfortable using Outlook encryption, she sent a test encrypted email to PO. PO's verification showed email was encrypted.

Complaint is considered closed as of 7/3/2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000105786
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	6/25/2014
Date Closed:	7/28/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0607491
Date US-CERT Notified:	6/25/2014
US-CERT Case Number:	INC000000379177
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

On 06/24/14 around 4:30 PM, a nurse from Amedisys (Home Healthcare agency) reported to the Privacy Officer (PO) that one of her clients who is a Veteran brought home six (6) different lab orders with a urine specimen belonging to another Memphis VAMC patient. According to the nurse, before she started dressing the Veteran's wound, she requested for his wound care supplies and Veteran pointed to a plastic bag lying in a corner in his room. She (nurse) opened the plastic bag and found six (6) lab orders with the urine specimen, all placed in the same plastic bag. The lab orders showed another Veteran's full name, DOB and full SSN. The Veteran stated to the nurse that the lab orders with the urine specimen were given to him by Memphis VAMC during his 06/18/14 clinic visit. The Veteran asked the nurse to discard the urine and lab orders. The nurse then discarded the urine in Veteran's bathroom and discarded the lab orders in one of the shredder lockboxes located at the Amedisys premises. The nurse stated she and the Veteran were the only persons who viewed the contents on the lab orders. She was in Veteran's house on 06/23/14 to provide patient care; and it was during this time she identified the lab orders and the urine specimen.

Incident Update

06/25/14:
The Incident Resolution Service Team determined that the 6 other Veterans will receive a letter offering credit protection services since their full SSNs were compromised.

06/26/14:
Per the PO, all 6 different lab slips were generated on the same Veteran, so only one Veteran was involved. The one Veteran will receive a letter offering credit protection services.

Resolution
PO met with two staff, Nursing Assistant and Chief of the SCI Outpatient clinic where the Veteran may have picked the urine specimen and lab orders belonging to another VA patient. The process of picking up and delivering lab specimen from SCI to Pathology and Lab has been reviewed. PO recommended a tracking system (spreadsheet) which will require all VA workforce picking up and delivering the specimens to Pathology and Lab sign-in to acknowledge pickup. After pickup, staff from SCI Outpatient Clinic will follow up to verify from Pathology and Lab to make sure specimens have been delivered as planned. During PO's review of the incident, he noted the affected Veteran's PII may have been inappropriately exposed, i.e. full name, SSN and DOB.

Credit monitoring letter has been prepared and mailed to the affected Veteran.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000105925
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	6/27/2014
Date Closed:	
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0607622
Date US-CERT Notified:	6/27/2014
US-CERT Case Number:	INC000000379801
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Veteran received a packaged mailed to her home address and after opening the box, she identified medication wrapped with name and address of another Veteran. She then called Telephone Care staff to report it. The PO has spoken with Veteran who is going to mail the package back to the Memphis VAMC. Complainant stated, the only PII she saw was full name and mailing address of the affected Veteran.

Incident Update

06/30/14:
The Incident Resolution Service Team has determined that Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

The fact-finding conducted into the incident by the Chief of Pharmacy indicated the medication package was mailed to the Veteran by the CMOP Pharmacy , located in Murfreesboro, TN. Veteran used to be seen here at Memphis VAMC and then moved without changing his mailing address . Memphis PO is transferring this incident out to CMOP Pharmacy Privacy Officer for follow up and remediation .

From Memphis side, there is not evidence of violation so complaint needs to be closed.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000106060
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	7/1/2014
Date Closed:	7/28/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Veteran reported to PO that during a visit to the Jonesboro CBOC on 6/27/2014, a Physician Assistant, met with him. Upon arrival at the CBOC, he waited for 45 minutes at the waiting area before being asked to go to an exam room to wait for a provider. According to Veteran, when the provider came to the exam room, she opened the door and asked him the reason for the visit. According to the Veteran, the provider was standing by the exam room door and was very loud when she spoke to him. Veteran stated further that while the provider was asking him series of questions about his clinic visit , he stood by the exam room door which was widely open and very close to the hallway. Veteran stated he was expecting that the provider would close the door to provide privacy safeguards to avoid inappropriate disclosure of his medical information. He stated two other patients who were passing in the hallway overheard the medical discussions because the provider was standing by the exam room door. Veteran is requesting the incident to be investigated because his personal privacy has been violated.

Based on the report, no PII was at risk; Veteran was concern about his PHI.

Resolution
PO and Contract CBOC Administrator have concluded their fact-finding on this complaint. Summary report provided by the CBOC Administrator indicated the Nurse Practitioner went into the exam room and shut the door. Shortly thereafter, her nose and eyes started to have severe burning due to odor from patient and his spouse. In order to be able to continue the office visit, the Nurse Practitioner opened the exam room door to allow air to circulate in the room. She noted that neither Veteran nor spouse raised any objections to the door being opened, nor did they ask for the door to be closed. Nurse Practitioner stated there was no exposure of PHI nor was a physical assessment exposed to anyone in the hall. Nurse Practitioner stated she is aware of auditory privacy issues, so she spoke in a quiet tone of voice to prevent medical discussions being over heard by others. Nurse Practitioner stated further that the visit was completed without objections or complaints from patient as alleged in his privacy complaints to Memphis VAMC PO.
When PO followed up again with patient, he insisted exam room door was opened but he did not raise any objections. When asked whether he notified any staff member from the clinic about violation of his privacy, he stated “no.”
Review of patient personal account of the complaint and the fact-finding report does not indicate privacy violation of any kind occurred as alleged by Veteran. PO noted what happened may have been incidental disclosure which the provider has been re-educated. PO stated in his report to CBOC Administrator that in order to prevent privacy breach arising from incidental disclosure, exam room doors must be closed at all times. If Provider has excusable reason for leaving exam room door open, this must be discussed with patient. The CBOC Administrator also requested Nurse Practitioner to review VA Privacy and HIPAA Focused Training to refresh her mind on patient privacy issues and how to prevent them from happening. PO noted this complaint did not result in any privacy breach.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000106388
Incident Type:	Unauthorized Electronic Access
Organization:	VISN 09 Memphis, TN
Date Opened:	7/10/2014
Date Closed:	7/14/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0608093
Date US-CERT Notified:	7/10/2014
US-CERT Case Number:	INC000000382582
Category:	Category 4- Improper Usage
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Veteran is alleging that another Veteran has been accessing her patient record . The complainant believes the other Veteran has memorized her social security number and is using it to access and look up the dates and times of her clinic appointments at the Memphis VAMC so that he may track her movements. Complainant notified one of Mental Health providers that the accused Veteran called her cell phone on Monday , July 7, 2014 and mentioned to her that she was not in attendance of Mental Health PRRC Group sessions on that date. When she (complainant) asked how he knew that information, the accused Veteran stated he heard this from complainant's friends who are also enrolled in the Mental Health PRRC program . It is believed that the accused Veteran is a Memphis VAMC.

Incident Update

07/14/14:
It has been confirmed that this individual (accused Veteran) is NOT a VA employee. He is an alumni of the Mental Health PRRC program. As an alumni, he has the privilege to come to the VAMC and attend Mental Health PRRC community and monthly meetings, and to socialize with current participants. Complainant and this individual may have been in a relationship before and for some reason, complainant is trying to sever the relationship.

At this time, it is not known how the accused person managed to get the SSN of complainant and used it to access VA systems to retrieve her information. Since the accused Veteran is not a VA employee there is no way to determine he accessed the VA systems to view and retrieved complainant 's information as alleged in the complaint. Complainant may have shared information with him previously; It is also possible complainant may have shared her MyhealtheVet login inormation with him previously but nobody can confirm this.

The Incident Resolution Team has determined that no breach has occurred.

Resolution
PO has followed up on this incident with staff from Mental Health Department to get additional information. It has been confirmed that this individual (accused Veteran) is NOT a VA employee. He is an alumni of the Mental Health PRRC program. As an alumni, he has the privilege to attend Mental Health PRRC community and monthly meetings, and socialize with current participants. Complainant and accused Veteran may have been in a relationship before and for some reason, complainant is trying to sever the relationship.

At this time, it is not known how the accused Veteran managed to get complainant's SSN to use it to access VA systems to retrieve her information. Since the accused Veteran is not a VA employee there is no way to determine the way and manner he accessed the VA systems to view and retrieved complainant 's information as alleged in the complaint. Complainant may have shared information with him previously; It is also possible complainant may have shared her MyhealtheVet login information with him previously but nobody can confirm this.

Complaint is not valid and is closed as of 7/11/2014. Complainant will be notified about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000106692
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	7/17/2014
Date Closed:	7/29/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Veteran was in Women's Clinic to meet with her Primary Care Provider (PCP) to request a medication refill. The assistant communicated the Veteran's request to PCP. According to the Veteran, she overheard the PCP telling the assisting nurse that the patient could not have a refill on pain meds and that she is 'drug seeking." Patient believes that his incident is a violation of her HIPAA privacy rights.

Resolution

This event was a clear violation by Dr. Chisholm of this Veteran's trust as well as the Mission of the Women's Program "to ensure all women Veteran's experience timely, equitable, high quality comprehensive health care in a sensitive and safe environment."

Fact-finding conducted by the Supervisor indicated the Veteran's PHI was mentioned and it was audible in the hallway . The PHI included type of medication, numerous personal details, and a stigmatizing judgment attached. The provider did not admit to revealing the patient's name (PII), but the witness (VA employee), heard the provider say the patient's name in the hallway .

PO has determined there is evidence of a breach of complainant's privacy and she feels she is being stigmatized by the event . PO has provided his summary report requesting the Supervisor to meet with HR to determine appropriate adverse action that can be taken to prevent future occurrence of the incident. The complainant will be notified about the outcome of the fact-finding. Complaint is considered closed as of 7/25/2014

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000107198
Incident Type:	Privacy
Organization:	VISN 09 Memphis, TN
Date Opened:	7/30/2014
Date Closed:	8/6/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Veteran reported to PO that on 7/23/2014, while he was in the waiting room at the Orthopedic Clinic a provider came in and spoke with him in a loud voice regarding his medication. He stated he provider said: "we are not going to give you any medication, it is too much." According to Veteran, his privacy has been violated because provider spoke very loudly and everybody in the waiting room heard the conversation.

Resolution

Provider comes to the VAMC once every week so PO scheduled time to meet with him today (8/6/2014) for fact-finding regarding this complaint.

Provider stated he was called during clinic from the front desk saying that the patient was asking why he received less pain medication than last time and asked to speak with him. Provider had seen the patient during his scheduled appointment approximately 2 days prior at which time he detailed his prescriptions. On the day in question, the patient (complainant) showed up unannounced without an appointment; he basically came in just to question about his prescription. Provider told the desk clerk that there was nothing to discuss but the patient insisted that provider should come and speak with him. In view of this provider come and stood by the waiting area entrance and as soon as he (patient) saw him, he volunteered his complaint that "he did not get as much pain medicine as he wanted." Provider then told him he would need to see his PCP if he desired more medication because it was not appropriate for orthopedic clinic to give more prescription. Patient became upset and repeatedly and loudly told provider to give him more pain medicine. Provider told him there was nothing to discuss as this was policy and he repeatedly requested more medicine. Provider replied patient that he was not going to have that discussion with him anymore. Provider told him several times there was nothing to discuss and he continued to become more upset. Provider therefore ended conversation as politely as possible while the patient continued to argue over the top of me. Meanwhile there were people in the waiting area who saw the patient talking loudly.

After fact-finding with provider, PO determined there was no violation because it was the patient (complainant) who volunteered a discussion on his medication in an open area. It was patient who initiated the conversation and insisted that provider should talk to him. Since patient knew about privacy requirements, he could have requested provider to speak with him privately to avoid discussions being overheard. Patient willingly discussed his prescription issues in an open area. PO also noted provider did not mention any name of medication neither referenced patient diagnosis.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000107673
Incident Type:	Non-VA Responsible/Non-Incident Upon Further Investigation
Organization:	VISN 09 Memphis, TN
Date Opened:	8/8/2014
Date Closed:	8/15/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Memphis VA Police during his routine patrol found a sheet of paper on the roadway close to the Emergency Room entrance . The was identified to be an outside hospital patient observation record which contains the name of the non- VA hospital, Veteran's name, date of birth and diagnosis. The roadway where the sheet was found is the spot where Ambulance Service usually pull up to get patients out to the ER .

Resolution

During PO's meeting with the Chief of ER for facting on the incident, he disclosed that the patient observation record sheet was brought in by Ambulance from a Behavioral Health System (non-VA facility) and was never handed over to Memphis VAMC ER staff. He stated if the sheet was handed to his staff, it would be impossible for it to be blown away from inside the ER through the main ER entrance to the roadway where it was found. He therefore stated, the ambulance staff may have mistakenly dropped the sheet of paper on the roadway and did not realize the error. PO determined that there was no violation arising from the incident for which Memphis VAMC is responsible. Complaint is considered closed as of 8/15/2014.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000107725
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	8/11/2014
Date Closed:	8/25/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	
Date US-CERT Notified:	N/A
US-CERT Case Number:	N/A
Category:	
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Spouse of a Veteran reported that Memphis VA Medical Center Mental Health Clinic Check-in staff has release her husband's appointment slip to a care-giver without appropriate authorization. Complainant stated even though the care-giver accompanied the couple to the hospital for clinic appointment, she did not have need to know of the information contained on the Veteran's clinic appointment slip.

Resolution

PO has concluded fact-finding on the complaint. The employee who was interviewed regarding the incident was truthful to provide details of the circumstances leading to the incident. Patient and wife came in to the clinic in the company of their care-giver; she noted they all sat close to each other. She assumed that it was in the best interest of the patient and wife to allow their care-giver to handle the Veteran's future appointment sheet. She stated that both Veteran and Wife saw her giving the sheet of paper to the care-giver and did not raise any objection.

The fact-finding occurred in the presence of employee's supervisor, a NAGE representative and facility Privacy Officer. PO educated employee that even though patient came to the clinic with his care-giver, she (employee) did not provide any objection to the patient whether it was in his best interest for the care-giver to handle his future appointment sheet. PO advised that, from now forward, employee should always seek verbal concurrence from patients before sharing their health information with their care-givers or any accompanying family member or friend. Employee verbalized understanding of PO's guidance. PO determined employee acted inappropriately and requested her supervisor to provide further training to avoid this type of incident from happening again. Complaint is considered closed on 8/25/2014; PO will notify complainant about the outcome of the fact-finding.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000108027
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	8/18/2014
Date Closed:	
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0609800
Date US-CERT Notified:	8/18/2014
US-CERT Case Number:	INC000000392577
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

An outside entity called and reported to Memphis VAMC Radiology Supervisor that they have received a fax pertaining to outpatient x -ray records meant to be faxed to another place. Complainant indicated that the fax contains patient full and SSN.

Incident Update

08/18/14:
The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services .

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number:	PSETS0000108368
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Memphis, TN
Date Opened:	8/26/2014
Date Closed:	
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0610131
Date US-CERT Notified:	8/26/2014
US-CERT Case Number:	INC000000394720
Category:	Category 6 - Investigation
Date OIG Notified:	N/A
Reported to OIG:	N/A
OIG Case Number:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An employee faxed a job application to USAjobs.gov and mistakenly included a VA patient tele-retina and appointment result sheet. The sheet included PHI and PII such as Veteran full name, address and eye test results.

DBCT Decision Date: N/A

DBCT:

Security Privacy Ticket Number: PSETS0000108373

Incident Type: Mishandled/ Misused Physical or Verbal Information

Organization: VISN 09
Memphis, TN

Date Opened: 8/26/2014

Date Closed:

Date of Initial DBCT Review: N/A

VA-NSOC Incident Number:

Date US-CERT Notified: N/A

US-CERT Case Number: N/A

Category:

Date OIG Notified: N/A

Reported to OIG: N/A

OIG Case Number: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

Chief of Pathology and Lab notified Privacy Officer that an unidentified individual had released VA Patient information to College of American Pathologists (CAP) as part of a plan to report the Service for patient care non-compliance. The Chief provided copy of a letter she received from CAP and it shows last names of three of the patients reported.

DBCT Decision Date: N/A

DBCT: