DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

October 24, 2014

The Honorable Carolyn N. Lerner
Special Counsel
U.S. Office of Special Counsel
1730 M Street, NW, Suite 300
Washington, DC 20036

RE: OSC File No. DI-14-0493

Dear Ms. Lerner:

I am responding to your letter regarding allegations made by a whistleblower at the G.V. (Sonny) Veterans Affairs (VA) Medical Center, (hereafter, the Medical Center) in Jackson, Mississippi. The whistleblower alleged that Medical Center employees violated patient privacy by accessing their medical records to create My HealtheVet accounts for them without their knowledge and that this may constitute a violation of law, rule, or regulation, and/or an abuse of authority. The Secretary has delegated to me the authority to sign the enclosed report and take any actions deemed necessary as referenced in 5 United States Code § 1213(d)(5).

The former Secretary referred the whistleblower's allegations to the Office of the Medical Inspector, Veterans Health Administration (VHA), which conducted a site visit to the Medical Center on May 7–8, 2014. VA substantiated the allegation that employees at the Medical Center repeatedly accessed the medical records of Veterans to obtain the personal information needed to create My HealtheVet accounts for Veterans without their knowledge. In addition, VA partially substantiated the allegation of a failure to properly notify Veterans of the intrusion and the allegation of improperly stored records at the Veterans Integrated Service Network (VISN) 16's Consolidated Fee Unit (CFU) in Pearl, Mississippi.

VA made three recommendations for the Medical Center, one for VHA, and one for the VISN/CFU. Findings from the investigation are contained in the report, which I am submitting for your review.

Thank you for the opportunity to respond.

Sincerely,

Jose D. Riojas
Chief of Staff

Enclosure

DEPARTMENT OF VETERANS AFFAIRS
Washington, DC

Report to the

Office of Special Counsel

OSC File Number DI-14-0493

Department of Veterans Affairs

G.V. (Sonny) Montgomery Veterans Affairs Medical Center

Jackson, Mississippi

Report Date: September 11, 2014

TRIM 2014-D-651

Executive Summary

The former Secretary directed the Office of the Medical Inspector (OMI) to investigate complaints lodged with the Office of Special Counsel (OSC) by (b)(6) (hereafter, the whistleblower), at the G.V. (Sonny) Montgomery Veterans Affairs (VA) Medical Center, in Jackson, Mississippi (hereafter, the Medical Center). The whistleblower alleged that employees at the Medical Center engaged in conduct that may constitute a violation of law, rule, or regulation, gross mismanagement, and an abuse of authority. He described issues regarding patient privacy and improper storage of VA information. OMI conducted a site visit to the Veterans Integrated Service Network (VISN) 16 Consolidated Fee Unit (CFU) in Pearl, Mississippi, on May 7–8, 2014.

Specific Allegations of the Whistleblower

1. Employees violated patients' privacy by directing staff to create My HealtheVet (MHV) accounts for patients without their permission;
2. Management failed to notify patients of the improper creation of the My HealtheVet accounts or take proper corrective action; and
3. Management violated patient privacy by allowing the improper storage of patient billing information and other personally identifiable information (PII) at the VISN 16 CFU in Pearl, Mississippi.

VA either **substantiated** allegations when the facts and findings supported that the alleged events or actions took place, or **did not substantiate** allegations when the facts showed the allegations were unfounded.

After careful review of OMI's findings, VA makes the following conclusions and recommendations.

Conclusions for Allegation #1

- VA substantiated the allegation that employees violated Veterans' privacy by directing staff to create MHV accounts for patients without their permission. Although there is no formal, written guidance that prohibits the practice of setting up accounts without the Veteran's authorization, the training provided to MHV coordinators set the expectation that staff were prohibited from creating MHV accounts for Veterans without their permission. The creation of these accounts by staff constitutes unauthorized access to protected health information (PHI) and is a violation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Privacy Act.

- While MHV training addressed the prohibition of staff members establishing MHV accounts for Veterans without their permission, a lack of written guidance contributed to the unauthorized establishment of these accounts.

Recommendations to the Medical Center

1. Provide specific training to ensure Medical Administration Service (MAS) staff understand VA and Veterans Health Administration (VHA) privacy policies and regulations related to safeguarding privacy. Monitor compliance and address noncompliance, as indicated.

2. Complete the actions approved in the Administrative Investigation (AI).

   - The Medical Center has provided documentation that it has completed Equal Employment Opportunity (EEO) and Privacy Training for the 19 supervisors who make up MAS Leadership during MAS supervisors' meetings on May 29, 2014, and June 6, 2014.

   - The Medical Center has provided documentation that it has completed four of the five disciplinary actions against employees who violated MHV privacy. The fifth disciplinary action is in progress. Specifically, for the five employees, the Medical Center Director has:

     a. Employee 1 – Proposed termination effective July 18, 2014; employee retired July 17, 2014.
     b. Employee 2 – Terminated, effective June 20, 2014.
     c. Employee 3 – Reassigned to another position and received a 30-day suspension; completed on June 30, 2014.
     d. Employee 4 – Proposed 7-day suspension with final decision to reduce suspension to 2 days; completed August 16, 2014, and August 17, 2014
     e. Employee 5 – Proposed 3-day suspension

Recommendation to VHA

3. Develop formal, written guidance for the MHV program (policy, handbook, or directive) to describe the entire MHV program including the account registration process. Make sure that employees are aware that they are forbidden from registering Veterans for MHV accounts without their permission.

Conclusions for Allegation #2

- VA substantiated the allegation that the Medical Center failed to notify Veterans of the improper creation of MHV accounts.

- VA did not substantiate the allegation that the Medical Center failed to take proper corrective action. We found that the Medical Center Director took appropriate managerial and disciplinary actions, as outlined in the AI.

Recommendation to the Medical Center

4. Send letters to all Veterans whose MHV accounts were established by VA employees without their knowledge or permission, informing them of the improper access.

Conclusions for Allegation #3

- VA substantiated the allegation that management allowed improper storage of patient billing information. Reasonable safeguards were not in place during the period when large amounts of paper records had to be temporarily stored at the CFU. The presence of unsupervised contract personnel, who had no need for access to the private information contained in the files temporarily stored in the CFU, and the potential for incidental disclosure necessitated consideration and implementation of additional reasonable safeguards during the temporary storage period.

- VA did not substantiate the allegation that the paper records were improperly secured. According to VISN 16 leadership, they were always kept behind a locked door.

- VA did not substantiate the allegation that Veterans' privacy was violated by the temporary storage practices at the CFU. Although reasonable safeguards were not in place to prevent incidental disclosure while the contracted janitor performed her duties, given the information obtained from CFU staff, we found no evidence that a member of the CFU staff or any other person inappropriately accessed Veterans' records.

Recommendation to VISN 16 and CFU Management

5. Develop appropriate, specific, and reasonable safeguards for the temporary storage of paper records to prevent incidental disclosure.

Summary Statement

VA found violations and apparent violations of VA and VHA privacy policy.

Table of Contents

I. Introduction

The former Secretary directed OMI to investigate complaints lodged with OSC by the whistleblower, a medical supply technician at the Medical Center, who alleged that employees at the Medical Center engaged in conduct that may constitute a violation of law, rule or regulation, gross mismanagement, and an abuse of authority. He described issues regarding patient privacy and improper storage of VA information. OMI conducted a site visit to the VISN 16 CFU in Pearl, Mississippi, on May 7–8, 2014.

II. Facility and VISN Profile

The Medical Center serves a population of over 45,000 unique Veterans, providing primary, secondary, and tertiary medical, neurological, and mental health inpatient care. It also operates a 120-bed community living center. To support its health education and physician residency programs, the Medical Center has affiliations with the University of Mississippi Medical Center, Alcorn State University, and three community colleges.

VISN 16, the South Central VA Health Care Network, covers an area of 170,000 square miles, serving Veterans in Oklahoma, Arkansas, Louisiana, Mississippi, and parts of Texas, Missouri, Alabama, and Florida. More than 445,000 Veterans seek care annually at VISN 16's ten medical centers and 40 community-based outpatient clinics.

III. Specific Allegations of the Whistleblower

1. Employees violated patients' privacy by directing staff to create MHV accounts for patients without their permission;
2. Management failed to notify patients of the improper creation of the MHV accounts or take proper corrective action; and
3. Management violated patient privacy by allowing the improper storage of patient billing information and other PII at the VISN 16 CFU in Pearl, Mississippi.

IV. Conduct of the Investigation

The original OMI team consisted of (b)(6) the Medical Inspector, and (b)(6) Clinical Program Manager. (b)(6) Deputy Medical Inspector, and (b)(6), Clinical Program Manager, assisted in the investigation after completion of the site visit. Because the complaint involved two different events, the investigation was divided into two efforts. The first effort involved allegations about the MHV program at the Medical Center. The second involved the VISN-operated CFU. For both efforts, OMI reviewed relevant policies, procedures, reports, memorandums, and additional documents as listed in Attachment A. Since the Medical Center had conducted both fact-finding and an AI of the MHV incident and has taken action based on the findings of these investigations, OMI only reviewed the documents generated by those investigations.

OMI interviewed the whistleblower by telephone prior to the site visit and conducted in-person interviews and teleconference calls with the following VA security and privacy experts to get a better understanding of the MHV program and its privacy and security implications:

- (b)(6) Whistleblower, the Medical Center
- (b)(6) Assistant Deputy Under Secretary for Health (ADUSH) for Informatics and Analytics, VHA
- (b)(6) Director, National Information Access and Privacy Office and VHA Privacy Officer, VHA
- (b)(6) Director, Incident Resolution Service, VA
- (b)(6) Director, Veterans/Consumers Health Informatics Office, VHA
- (b)(6) Deputy Director, Veterans/Consumers Health Informatics Office, VHA
- (b)(6) Information Security Officer, the Medical Center
- (b)(6) My HealtheVet Coordinator, the Medical Center

OMI conducted a site visit to the VISN 16 CFU in Pearl, Mississippi, on May 7–8, 2014. During this site visit, OMI held entrance and exit briefings with VISN leaders and CFU managers and toured the facility.

OMI interviewed the following individuals:

- (b)(6) VISN 16 Deputy Network Director
- (b)(6) VISN 16 Associate Deputy Network Director
- (b)(6) VISN 16 Chief Fiscal Officer
- (b)(6) VISN 16 Business Implementation Manager
- (b)(6) VISN 16 Privacy Officer
- (b)(6) Scanner/Mail Clerk
- (b)(6) Non-VA Medical Bill Claims Processor
- (b)(6) Distribution Clerk
- (b)(6) CFU Clinical Manager
- (b)(6) CFU Office Manager
- (b)(6) Non-VA Medical Bill Claims Processor
- (b)(6) CFU Non-VA Medical Bill Appeals Clerk
- (b)(6) Telephone Operator
- (b)(6) Telephone Operator
- (b)(6) Scanner/Mail Clerk
- (b)(6) Non-VA Medical Bill Claims Processor
- (b)(6) Non-VA Medical Bill Claims Processor
- (b)(6) (b)(6) Lead Non-VA Medical Bill Claims Processor
- (b)(6) Clinical Coordinator

The Office of General Counsel reviewed VA's findings to determine whether there was any violation of law, rule, or regulation.

V. Findings, Conclusions, and Recommendations

Allegation 1: Employees violated patient's privacy by directing staff to create My HealtheVet accounts for patients without their permission.

Findings

The MHV Web site (www.myhealth.va.gov) is designed for Veterans and their families to optimize Veterans' health and is available to Veterans, Servicemembers, dependents, caregivers, health care providers, and advocates. It currently serves 2.7 million Veterans nationwide. To provide a secure, accessible, personal health record for Veterans, MHV offers Veterans the ability to complete the following tasks:

- Refill VA prescriptions online;
- Track and monitor important, self-entered vital signs and other personal data;
- View VA appointments and laboratory results;
- Obtain copies of key portions of VA health records;
- Manage health goals; and
- Use secure messaging to communicate electronically with VA health care teams.

Veterans can register for one of the three types of MHV accounts: Basic, Advanced, and Premium. Veterans may register for a Basic MHV account without providing their Social Security Numbers (SSN), in order to enter health metrics they have obtained from VA and other sources such as blood sugar, weight, laboratory results, access to trusted health libraries, and a health assessment tool; this type of MHV account does not provide the Veteran access to PHI. Registration for Advanced or Premium accounts requires input of the Veterans' SSNs, gives Veterans access to PHI, offers the ability to request VA prescription refills, and view selected information in their VA and Department of Defense records.

Anyone opening an MHV account must have Veteran Sensitive Personal Information (SPI), which includes the individual's name, address, and phone number in combination with other information that can be used to distinguish or trace the individual's identity, such as the SSN and birthdate.[1] Under HIPAA, a Veteran's SPI is a type of PHI when this information is included with health information in the medical record. The HIPAA Privacy Rule, 45 Code of Federal Regulation (CFR) §§ 160.103, requires that covered entities, including VHA, "ensure confidentiality ... of all electronic protected health information."[2] Confidentiality includes preserving authorized restrictions on information access and disclosure. If unauthorized access occurs, the breach notification rule requires patient notification for certain incidents involving access to, or disclosure of,

[1] VA Handbook 6502 defines "Sensitive Personal Information" (as defined in VA Handbook 6500) as any information about the individual maintained by an agency, including the following: (i) education, financial transactions, medical history and criminal, or employment history; (ii) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric record.
[2] HIPAA Privacy Rule. http://www.hhs.gov

PHI in a manner not permitted under the HIPAA Privacy Rule. In addition, the VA Information Security Enhancement Act of 2006, 38 United States Code (U.S.C.) § 5724(a)(2), requires "[i]f the Secretary determines ... that a reasonable risk exists for the potential misuse of SPI involved in a data breach, the Secretary shall provide credit protection services." Credit protection services include notification of the affected Veterans.

The person completing the registration process for a Basic MHV account must enter the following information into the electronic registration form:

- First and last name;
- Gender;
- Birth date;
- An indication of the status of the person completing the registration form (from the following list: VA patient, Veteran, health care provider, Veteran advocate/family member/friend, VA employee, or other);
- Address;
- Preferred method of contact;
- Account user identification and password; and
- Two hint questions with answers in order to reset the account user identification or password.

Although the registration page asks the Veteran to enter the SSN, this is not required for opening Basic accounts, only for Advanced or Premium accounts. In addition, the Veteran must agree to MHV terms and conditions and VA's privacy policy, as set forth by VA for use of the account, by checking two boxes on the registration page. Veterans cannot be registered for an MHV account unless they agree to the terms and conditions of use. Agreement to the terms and conditions by anyone other than the Veteran is considered an impersonation of that Veteran.

There is no formal written guidance, such as a VHA directive or handbook, that describes the MHV program and the authorization and procedures required for setting up accounts. VHA Handbook 1907.02, *My HealtheVet In-Person Authentication*, provides guidance on how to perform in-person authentication for Veterans with an Advanced and Premium MHV account, both of which permit access to individually-identifiable health information. VHA has trained MHV coordinators in the appropriate method for establishing MHV accounts. The training, titled "Avoid Trouble by Knowing Your My HealtheVet Role and Responsibilities" was presented to MHV Coordinators in January 2013. The training specifically instructed them not to create MHV accounts for Veterans without their permission, and that the creation of these accounts by them would be considered unauthorized access to PHI. This training also described how agreeing to terms and conditions for the account by staff members without the permission of the Veteran constituted an impersonation of the Veteran. Finally, VA's National Rules of Behavior state "... unauthorized access ... to information on VA systems is prohibited."

On March 1, 2013, the MHV Help Desk at the Medical Center received a complaint from a Veteran about a letter informing him that the Medical Center had signed him up for an MHV account. He reported that he had never visited the Web site, nor had he signed up at the facility. The Veteran read the letter to the Help Desk representative. The letter referenced user identification and hint questions to allow password changes, as well as instructions on how to access and complete the self-help password reset function. The Veteran stated that the hint questions to reset the password were not relevant to him.

On March 4, 2013, the Medical Center reported this incident to the VA Network Security Operations Center (VANSOC) and entered it into the Privacy Security Event Tracking System (PSETS) for evaluation of a possible breach of SPI, as required by VA Handbook 6502.1, *Privacy Event Tracking,* where the possibility of a breach of SPI exists.[3] On March 8, 2013, the Medical Center discovered that an additional 24,215 Veterans had been registered for Basic MHV accounts by VA employees rather than by Veterans themselves. Concerned that the registration of these Veterans was a data breach, the incident was referred, as required by VA Handbook 6500.2, to the weekly Data Breach Core Team (DBCT) meeting to determine whether this incident was a breach of SPI.

The Medical Center's investigation also revealed that an internal project to register Veterans into MHV to increase enrollment numbers began in May 2012 and continued until the end of February 2013. Medical Center employees opened the MHV Web site, and prepared the registration application using PHI data extracted from the Veterans Health Information Systems and Technology Architecture (VistA). This information included the Veteran's first and last name, social security number, date of birth, and gender. The employee then created a user identification and password, accepting the MHV Web site's "Terms and Conditions" and "Privacy Policy" for the Veteran who had just been registered. This action constitutes an impersonation of the Veteran, since only the Veteran is expected to accept terms and conditions for the account. The intent of the project was to facilitate Veterans' registration into MHV so that they could upgrade to an Advance or Premium account at their next appointment to take advantage of the enhanced level of benefits more quickly. Between December 2012 and February 2013, the Medical Center sent letters to the Veterans who had been registered in this manner informing them that they had been registered into the program.

VA defines a data breach as the loss, theft, or other unauthorized access to SPI data, other than those accesses incidental to the scope of employment, where such access results in the potential compromise of the confidentiality or integrity of the data. See 38 U.S.C. § 5727. The HITECH ACT (Health Information Technology for Economic and Clinical Health Act) defines a breach as the "unauthorized acquisition, access, use, or

[3] VA Handbook 6500.2 defines "Sensitive Personal Information" as individually identifiable information protected by one or more confidentially provisions such as the Privacy Act, 5 U.S.C. § 552a; 83 U.S.C. § 5701, 5705, and 7332; or the HIPAA Privacy Rule. Protected health information and personally identifiable information are subsets of SPI.

disclosure of protected health information which compromises the security or privacy of such information, except where an authorized person to whom such information is disclosed would not have reasonably have been able to retain such information." 42 U.S.C. § 17921(1). The Department of Health and Human Services (HHS) interim data breach notification regulations in effect when the incident occurred clarified that "compromises the security of privacy of such information," is limited to those instances where there is a "significant risk of financial, reputational, or other harm to the individual." 45 CFR § 164.402 (2010) (interim final regulation).[4]

On March 19, 2013, the DBCT determined that the incident did not meet the definition of a data breach. Because the incident was not judged a breach, there was no requirement, under law, regulation, VA Handbook 6500.2, or other policy, for the Medical Center to send Veterans a letter outlining breach remediation, such as an offer of credit monitoring. The Medical Center did not send these Veterans letters informing them of the unauthorized creation of their MHV accounts. The DBCT categorized the incident as unauthorized electronic access to SPI with low risk of compromise and with no further action required on their part. The National Information Access and Privacy Office (NIAPO) found that employee's unauthorized electronic access to Veterans' electronic health records to retrieve demographic data to create MHV accounts did qualify as a violation of VHA's privacy policy.[5]

Based on the original complaint and the initial fact finding, the Medical Center Director chartered an AI on June 14, 2013, to investigate allegations of a hostile work environment, privacy violations pertaining to MHV, and abuse of authority. The Board consisted of three investigators with relevant subject matter expertise brought in from other facilities to interview 46 witnesses. The Board substantiated that two MAS supervisors did create a hostile work environment, substantiated that the process used by the MAS to create MHV accounts did violate Veterans' privacy, but it did not substantiate an abuse of authority. The Board made 10 recommendations, three of which pertained to MHV, including the following actions by the Medical Center Director:

- Consider refresher privacy training for all MAS employees;
- Consider providing training to MAS managers on the requirements to stay after duty hours for completion of required work; and
- Consider taking administrative and/or disciplinary action against eight different employees.

[4] The final regulations were promulgated by HHS in January 2013, and effective September 23, 2013. See Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules: Final Rule, 78 Fed. Reg. 5566-5702 (January 25, 2013). Therefore, they were not in effect during the time that the improper accounts were being created and are not relevant to this report.
[5] VHA Handbook 1605.1, *Privacy and Release of Information,* paragraphs 3a.(1); 3b.(1) and (5); and 12a. provides guidance. VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information, paragraphs 5a., 6a., and 6b.

For five of the eight employees, the Board recommended administrative or disciplinary action for the privacy violation pertaining to the MHV allegation. The AI was signed by its members on October 3, 2013, and October 4, 2013, and all 10 recommendations were approved by the Medical Center Director on October 22, 2013.

Conclusions for Allegation #1

- VA substantiated the allegation that employees violated Veterans' privacy by directing staff to create MHV accounts for patients without their permission. Although there is no formal, written guidance that prohibits the practice of setting up accounts without Veterans' authorizations, the training provided to MHV coordinators set the expectation that staff were prohibited from creating MHV accounts for Veterans without their permission. The creation of these accounts by staff constitutes unauthorized access to PHI and is a violation of the HIPAA Privacy Rule and the Privacy Act.

- While MHV training addressed the prohibition of staff members establishing MHV accounts for Veterans without their permission, a lack of written guidance contributed to the unauthorized establishment of these accounts.

Recommendations to the Medical Center

1. Provide specific training to ensure MAS staff understand VA and VHA privacy policies and regulations related to safeguarding privacy. Monitor compliance and address noncompliance as indicated.

2. Complete the actions approved in the Administrative Investigation (AI).

    - The Medical Center has provided documentation that it has completed EEO and Privacy Training for the 19 supervisors who make up MAS leadership during the MAS supervisors meeting on May 29, 2014, and June 6, 2014.

    - The Medical Center has provided documentation that it has completed four of the five disciplinary actions against employees who violated MHV privacy. The fifth disciplinary action is in progress. Specifically, for the five employees, the Medical Center Director has completed the following actions:

        a. Employee 1 – Proposed termination effective July 18, 2014; employee retired July 17, 2014
        b. Employee 2 – Terminated, effective June 20, 2014
        c. Employee 3 – Reassigned to another position and received a 30-day suspension; completed June 30, 2014
        d. Employee 4 – Proposed 7-day suspension with final decision to reduce suspension to 2 days; completed August 16, 2014, and August 17, 2014
        e. Employee 5 – Proposed 3-day suspension

Recommendation to VHA

3. Develop formal, written guidance for the MHV program (policy, handbook, or directive) to describe the entire MHV program including the account registration process. Make sure that employees are aware that they are forbidden from registering Veterans for MHV accounts without the Veteran's permission.

Allegation 2: Management failed to notify patients of the improper creation of the My HealtheVet accounts or take proper corrective action.

Findings

The Medical Center did not send a notification letter offering credit monitoring to the Veterans involved, as the DBCT found that the incident was not a data breach. The letters sent to Veterans between December 2012 and February 2013, informed them that they had been registered in MHV but did not mention that registration occurred without their knowledge or permission, or contrary to VHA policy. The Medical Center did not send letters informing Veterans that their privacy had been violated without their knowledge. Since there is no VA or VHA policy requiring a courtesy letter, the Medical Center had the sole discretion to decide whether to send such a letter to each Veteran who had an MHV account opened for them. The current head of the MHV program at the Medical Center says she has had about five complaints in the year that she has been in this position; she also said that many Veterans involved have chosen to keep their accounts open and to use them.

By February 2013, the Medical Center had registered most of the eligible Veterans in MHV. By the time the complaint was lodged with the MHV Help Desk and the Medical Center, Veteran registration through this program had been completed, so Medical Center leadership did not have to take action to terminate the registration process. As discussed above, the Medical Center did convene an AI and implemented its recommendations.

Despite the low number of complaints received, the continued use of these MHV accounts, and the fact that notification is not required by law, regulation, VA Handbook 6500.2, or other policy, unauthorized access to Veterans' PHI occurred, resulting in a violation of the HIPAA Privacy Rule and the Privacy Act. The Medical Center should have informed Veterans of these violations.

Conclusions for Allegation #2

- VA substantiated the allegation that the Medical Center failed to notify Veterans of the improper creation of MHV accounts.

- VA did not substantiate the allegation that the Medical Center failed to take proper corrective action. We found that the Medical Center Director took appropriate managerial and disciplinary actions, as outlined in the AI.

Recommendation to the Medical Center

4. Send letters to all Veterans whose MHV accounts were established by VA employees without the Veteran's knowledge or permission, informing them of the improper access.

Allegation 3: Management violated patient privacy by allowing the improper storage of patient billing information and other personally identifiable information (PII) at the Veterans Integrated Service Network (VISN) 16 Consolidated Fee Unit in Pearl, Mississippi.

Findings

Located in Pearl, Mississippi, since 2007, the VISN 16 CFU is responsible for processing non-VA medical claims (bills) for all 10 VISN 16 medical centers. In fiscal year (FY) 2013, the CFU scanned and uploaded 922,105 such claims from over 7,500 health care providers and vendors, representing non-VA medical care for approximately 87,000 unique Veterans.

Although 133 full-time employee equivalent slots are assigned to the CFU, it currently has 94 VA employees divided among four units:

- Fee Payment – Processes non-VA medical claims.
- Fee Customer Service – Includes the call center and services the mailroom and scanning functions.
- Clinical Coordination – Nurses of the Clinical Coordination Unit perform clinical reviews of the medical bills, particularly for previously unauthorized and Millennium Bill claims.[6]
- Evening Unit – Created in June 2013, this group improves the timeliness of non-VA medical bill claims processing, and while claims processing is currently up-to-date, it continues to provide services for claims verification, claims distribution, authorization, mailroom, and scanning activities.

Processing non-VA medical care claims follows a data flow model. Documents received from non-VA health care providers are captured, indexed, and stored electronically. Some bills are submitted electronically; paper bills or claims for health care services are scanned and uploaded. All are verified to ensure the bill reflects the actual services provided. When the services are married to the billing documents and verified, they are coded and entered into a distribution module. This step processes the bill or claim, looking at authorization and eligibility. The claims may be sent for clinical

[6] VA is authorized under Title 38 U.S.C. 1725 to make payment or reimbursement for emergency treatment provided to a Veteran for a non-service connected condition, although VA must be the payer of last resort. VA may reimburse or pay claimants for non-VA emergency medical treatment to an eligible Veteran on and after May 29, 2000. The basic authorities and payment methodologies to provide unauthorized medical care are contained in 38 U.S.C. 1725 and 38 CFR 17.1000-17.1008. Retrieved from http://www.nonvacare.va.gov/millbill.asp.

review. Upon payment determination, the bill is either paid, rejected, or more information is requested.

In June 2012, the CFU began to experience delays in the non-VA care claims processing through the Fee Basis Claim System (FBCS), noting latency, timing out, and errors.[7] In July 2012, the FBCS developers indicated the latency was due to the age of the servers and user volume at any given time. Latency is critical in document processing, as it represents how quickly all of the objects on a form can appear on the computer screen. A reasonable goal is to have an entire page load in less than 3 seconds. Because these delays were creating a backlog of non-VA medical care claim processing, VISN 16 leadership requested guidance and assistance from the National Non-VA Medical Care Program Office (NNPO) and the Office of Information & Technology (OI&T).

In August 2012, NNPO staff validated the latency issue and made minor modifications to the server. OI&T reported there were no funds for a replacement server. In September 2012, due to continued server issues, the CFU had to cease scanning documents, resulting in a manual review of records and on-site storage of claims and files. Following a catastrophic failure of the FBCS server in July 2013, VISN 16 leadership approved purchase of a new server. In December 2013, the new server was installed, and for the next 3 months, CFU staff participated in overtime work to scan documents and claims into it. The CFU Business Manager reported that, as of May 2014, all backlogged mail and records had been scanned into FBCS or the document management system, resulting in improved timeliness in processing. The photos accompanying the allegations accurately reflect the situation in the CFU while it could not scan documents and had to manually review and store them. OMI did not observe any inappropriately stored patient billing information or PII during the site visit.

The CFU is housed in a two-story building with no exterior building signs or rosters to provide information about building occupants. The second story is home to a private corporation and another Federal agency.

The CFU occupies the entire ground floor of the building, with discreet hand painted signage on each door, indicating that it is a VA office. Each CFU employee is provided with a key to access the facility. No one can enter without a key or without assistance from an individual opening the door from the inside. A receptionist at the front door requires identification and the purpose of the visit from any non-employee seeking entrance. The doors are locked 24 hours per day, 7 days per week, with an automatic alarm system notifying the local police department of any unauthorized entry after duty hours or on weekends. The system was tested once when two supervisors failed to reset the alarm when entering. The building was surrounded by local police cars within minutes.

[7] Latency is the amount of time it takes for the host server to receive and process a request for a page object. The amount of latency depends largely on how far away the user is from the server. Retrieved from http://www.webperformancetoday.com/2012/04/02/latency-101-what-is-latency-and-why-is-it-such-a-big-deal/.

Within the building, a motion detector alarm system is operational during non-working hours; this also alerts the local police. Only VISN or CFU employees are present in the CFU. The CFU's strict policy requires that family or friends remain sequestered in the reception area during visits; contractors are escorted. There are no records or computer screens visible from the reception area. Within the CFU are specific modular work stations and larger areas for mail processing and scanning. The unit contains a large employee break room and kitchen. OMI observed document security procedures through all phases of processing documents and claims. Documents are scanned daily, and originals are placed in locked shredding containers. A contracted shredding company arrives weekly to process and remove shredding containers, which are unlocked, the contents transferred to a truck on the premises, and destroyed – all in a hands-free process. The truck does not depart the CFU until all documents are shredded.

Gateway Development, Inc., the lessor for the property, furnishes cleaning services for the CFU. One female housekeeper whose job is to clean the CFU on a daily basis, performs this task 5 nights a week. She has been the only housekeeper for the CFU since it moved into the facility. OMI found no evidence of privacy or security violations or concerns related to the housekeeper. No CFU employees reported any privacy or security concerns regarding the housekeeper, and indeed, stated that she will not even let them into the building after hours if they do not have their keys. VA Directive and Handbook 6500 § 71 states, "Contractors who are users of VA data and have authorized access to VA sensitive information and information systems should complete VA-approved security and privacy training and sign a VA Contractor Rules of Behavior." The housekeeper has not received VA privacy and security training. This training is not required by the terms of the building lease because, as a housekeeper, she would not need access to VA information and information systems to perform her duties. However, CFU leadership has decided to make arrangements with the lessor to provide VA privacy and security training to this housekeeper.

OMI interviewed CFU staff from all work sections and from both shifts, along with training documents for all CFU staff; 100 percent of employees are current with required VA training on privacy and security. No CFU employees reported privacy or security breaches within or related to the facility. On April 22, 2014, the VISN 16 Privacy Officer conducted by a privacy and security walk-through review of the CFU property and discussed results with CFU managers. Together, they developed an action plan to enhance CFU security and privacy. Action items include the following:

- Placing privacy and security awareness posters in the common areas and breakroom;
- Wearing identification badges within the unit;
- Exploring options for closed-circuit monitoring of the entryways; and
- Providing privacy screens for employees on the window side of the building (although the windows are tinted and curtains usually drawn).

OMI queried the VISN 16 Privacy Officer on the security status of the CFU premises. Because the CFU temporarily houses PII and PHI, VHA Handbook 1907.01, *Health Information Management and Health Records,* issued September 19, 2012, requires that health records in file areas be locked and that the facility control physical access by authenticating visitors before access to areas other than those that are publicly accessible. VA Handbook 0730, *Security and Law Enforcement,* issued August 11, 2000, (Appendix B), describes a controlled area as a space or area that has a minimum of single-barrier protection. VA Directive 6371, *Destruction of Temporary Paper Records,* issued April 8, 2014, prescribes processes for storage and destruction of temporary records, requiring reasonable physical safeguards to protect VA records during their transportation, transfer, or short-term storage prior to the completion of their final destruction. The VISN 16 Privacy Officer states that the current practice of keeping all exterior doors locked at all times meets the requirements for a controlled area.

However, HIPAA Privacy Rule (45 CFR 164.502(a)(1)(iii)) - *Incidental Uses and Disclosures and Reasonable Safeguards* requires the application of more stringent safeguards:[8]

> A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. See 45 CFR 164.530(c). It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all potential risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the PHI it holds, and assess the potential risks to patients' privacy. Covered entities should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards. Many health care providers and professionals have long made it a practice to ensure reasonable safeguards for individuals' health information – for instance by taking the following actions:
>
> - Speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;
> - Avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
> - Isolating or locking file cabinets or records rooms; or
> - Providing additional security, such as passwords, on computers maintaining personal information.

[8] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html

Further, as outlined in VHA Privacy Office, Privacy Fact Sheet, *Business Associate Agreement and their Applicability to Janitorial, Shredding, Hazardous Waste Disposal and Courier Services*, issued June 2014, janitorial service vendors who clean the offices or facilities of a covered entity are not considered to be business associates because the work performed for covered entities does not require them to use or disclose PHI. The fact that the janitorial service is performed after normal business hours and without VA supervision does not meet the HIPAA requirements for a business associate relationship, as the contractor does not need PHI to perform its janitorial services. In this instance, the employee performing janitorial services contracted to the CFU does not require the use or disclosure of PHI, is not a business associates, and therefore, does not need privacy or HIPAA training.

According to the NIAPO, while the janitors servicing the CFU without direct VA supervision after hours do not need privacy training required of business associates, the CFU must implement reasonable safeguards appropriate to the storage of its records while the janitor works unsupervised. Per the NIAPO, an example of a reasonable safeguard in this instance would be limiting janitorial services to duty hours while VA personnel are on-site to assure record confidentiality. Other acceptable reasonable safeguards would be boxing the records and insuring the boxes are taped shut every night or placing boxes in a locked closet to which the janitor does not have access.

Conclusions for Allegation #3

- VA substantiated the allegation that management allowed improper storage of patient billing information. Reasonable safeguards were not in place during the period when large amounts of paper records had to be temporarily stored at the CFU. The presence of unsupervised contract personnel, who had no need for access to the privacy information contained in the files temporarily stored in the CFU, and the potential for incidental disclosure necessitated consideration and implementation of additional reasonable safeguards during the temporary storage period.

- VA did not substantiate the allegation that the paper records were improperly secured. According to VISN 16 leadership, they were always kept behind a locked door.

- VA did not substantiate the allegation that Veterans' privacy was violated by the temporary storage practices at the CFU. Although reasonable safeguards were not in place to prevent incidental disclosure while the contracted janitorial staff performed their duties, given the information obtained from CFU staff and information reviewed, we found no evidence that a member of the CFU staff or any other person inappropriately accessed Veterans' records.

Recommendation to VISN 16 and CFU Management

5. Develop appropriate, specific, and reasonable safeguards for the temporary storage of paper records to prevent incidental disclosure.

Summary Statement

VA found violations or apparent violations of VA and VHA privacy policy.

Glossary

Data breach: VA Handbook 6500.2, *Management of Data Breaches Involving Sensitive Personal Information (SPI),* Jan 6, 2012.

(1) The VA-specific definition of the term "data breach" in 38 U.S.C. § 5727(4)1 is "the loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing SPI, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data."

(2) OMB Memorandum M-07-16, *Safeguarding against and Responding to the Breach of Personally Identifiable Information*, issued May 22, 2007, uses the term "breach." Footnote 5 of the Memorandum explains that "the term 'breach'" is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic." The OMB Memorandum specifically states that a breach occurs when: "An individual gains logical or physical access without permission to a Federal agency network, system, application, data, or other resource; or there is a suspected or confirmed breach of PII regardless of the manner in which it might have occurred."

(3) The HITECH ACT (Health Information Technology for Economic and Clinical Health Act) defines a breach as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an authorized person to whom such information is disclosed would not have reasonably have been able to retain such information." 42 U.S.C. § 17921(1).

(4) Interim regulations promulgated by the Department of Health and Human Services (HHS) clarify that "compromises the security of privacy of such information," is limited to those instances where there is a "significant risk of financial, reputational, or other harm to the individual." 45 C.F.R. § 164.402 (2010) (interim final regulation). It is unclear whether the final regulations will include this risk threshold, which is higher than the "reasonable risk of potential misuse" standard under 38 U.S.C. § 5724.

(5) While the three definitions of a data breach (or breach) use slightly different phrasing, they generally refer to unauthorized access to sensitive personal Information that results in the potential compromise of the confidentiality or integrity of the information. Consequently, the VA DBCT uses the VA-specific term, data breach, and its definition in determining whether the reported event constitutes a data breach that the DBCT reviews to decide whether VA has to notify the record subjects of the event and offer them credit protection services.

Data Breach Core Team: The DBCT is chaired by the Director, Incident Resolution Service, within the Office of the Deputy Assistant Secretary for Information Security.

The DBCT has oversight responsibilities for data breaches which it adjudicates to determine impact and reporting requirements. It is a matrix structure from the local to the national level that operates both vertically and horizontally.

Sensitive Personal Information (SPI): Information that: (1) is maintained by an agency; (2) is about an individual, such as education, financial transactions, medical history, protected health information, and criminal or employment history, and information that can be used to distinguish or trace the individual's identity (Personally Identifying Information – PII), including name, social security number, date, and place of birth, mother's maiden name, or biometric records; and (3) requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. Includes records about individuals requiring protection under applicable confidentiality provisions.

Personally Identifiable Information (PII): Any information which can be used to distinguish or trace an individual's identity such as name, SSN, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date, and place of birth, mother's maiden name, etc. (See SPI above).

Protected Health Information (PHI): Health (including demographic) data that is transmitted by, or maintained in, electronic or any other form or medium, and relates to: (1) the past, present, or future physical or mental health, or condition of an individual; (2) provision of health care to an individual; or (3) past, present, or future payment for the provision of health care to an individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

Information that: (1) is maintained by a covered entity, such as a health care provider or a health plan; (2) relates to the past, present, or future physical or mental health, or condition of an individual, the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (3) identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

VistA: The Veterans Health Information Systems and Technology Architecture (VistA) is an enterprise-wide information system built around the electronic health record used in VHA. It consists of nearly 200 integrated software modules for clinical care, financial functions, and infrastructure.

Attachment A
Documents Reviewed by OMI

1. Department of Veterans Affairs, VA Handbook 6500.2, January 6, 2012, *Management of data breaches involving sensitive personal information (SPI).*

2. Department of Veterans Affairs, VA Handbook 6502.1, February 18, 2011, *Privacy Event Tracking,*

3. Department of Veterans Affairs, VA Handbook 0730, August 11, 2000, *Security and Law Enforcement,* (Appendix B).

4. Department of Veterans Affairs, VA Directive 6066, April 2, 2008, *Protected Health Information.*

5. Department of Veterans Affairs, VA Directive 6371, April 8, 2014, *Destruction of Temporary Paper Records.*

6. Veterans Health Administration, VHA Directive 1605, April 11, 2012, *VHA Privacy Program.*

7. Veterans Health Administration, VHA Handbook 1907.01, September 19, 2012, *Health Information Management and Health Records.*

8. Veterans Health Administration, VHA Handbook 1907.02, June 27, 2008, *My HealtheVet in-person authentication.*

9. Veterans Health Administration, VHA Handbook 1907.06, January 13, 2013. *Management of Release of Information.*

10. Veterans Health Administration, VHA Handbook 1605.2, January 23, 2013, *Minimum necessary standard for protected health information.*

11. Veterans Health Administration, VHA Directive 1601, January 23, 2013, *Non-VA Medical Care Program.* Retrieved from http://nonvacare.hac.med.va.gov/docs/VHA-Directive-1601.pdf.

12. Veterans Health Administration, VHA Directive 2010-005, January 27, 2010, *Timeliness standards for processing non-VA provider claims.* Retrieved from http://nonvacare.hac.med.va.gov/docs/Timeliness_Standards_for_Processing_Non-VA_Provider_Claims.pdf.

13. Department of Veterans Affairs, Veterans Health Administration, *Notice of Privacy Practices.* Effective, September 23, 2013.

14. National Non-VA Care Policy & Procedures, http://nonvacare.hac.med.va.gov/policy-programs/.

15. Veterans Health Administration, Office of Health Data and Informatics, January 2009, *Privacy Fact Sheet: Use and/or access of protected health and individually identifiable information by VHA employees 9*(3).

16. Veterans Health Administration, Office of Health Information, February 2010, *My Health, My Care: 24/7 Online Access to VA, Improving 2-way communication. Retrieved from www.myhealth.va.gov.*

17. Veterans Health Administration, *My* HealtheVet, https://www.myhealth.va.gov/index.html.

18. VHA Privacy Office, Privacy Fact Sheet, June 2014, *Business Associate Agreement and their Applicability to Janitorial, Shredding, Hazardous Waste Disposal and Courier Services.*