DEPARTMENT OF VETERANS AFFAIRS
Office of the General Counsel
Washington DC 20420

FEB 10 2012

In Reply Refer To:

The Honorable Carolyn N. Lerner
Special Counsel
U.S. Office of Special Counsel
1730 M. Street, N.W. Suite 300
Washington, DC 20036-4505
Attn: Catherine A. McMullen, Chief, Disclosure Unit

Re: OSC File No. D1-11-2679 and D1-11-2798

Dear. Ms. Lerner,

We hereby provide your office with the enclosed redacted version of the Agency's response to allegations reported by an employee/Veteran and the employee's supervisor at the Department of Veterans Affairs Boston Healthcare System (VABHS), Brockton Division (Brockton), Business Office, Brockton, Massachusetts (OSC File No. D1-11-2679 and DI-11-2798). .

Under the Freedom of Information Act (FOIA), we would, at a minimum, analyze a report of this nature under exemptions (b)(6) and (b)(7)(C). Exemption (b)(6) requires that an agency determine whether disclosure "would constitute a clearly unwarranted invasion of personal privacy" by balancing the privacy interest that would be compromised by disclosure against the public interest in the requested information. Exemption 7(C) protects law enforcement information the disclosure of which "could reasonably be expected to constitute an unwarranted invasion of personal privacy."

Clearly the public has an interest in knowing how its government operates and that wrongdoing is addressed adequately. However, It has been held that career public servants retain personal privacy interests in the discharge of their public duties. New England Apple Council, Inc. v. Donovan, 725 F.2d 139 (1st Cir. 1984). This is particularly true in cases involving the investigation of alleged wrongdoing, as in this case. Federal employees also have personal privacy interests when disclosure of their identities could lead to harassment. In particular, the employees accused of the alleged infractions are mid-level and low-level employees. The investigation did not substantiate the whistleblowers' allegations that the named employees improperly accessed the employee/Veteran's full medical record or that management failed to take appropriate action. With regard to the investigation's additional findings, the individual involved also is a low-level employee, and management has taken corrective action. The employees who were interviewed for purposes of this investigation also are rank and file employees. The cooperation of rank and file employees is needed in any

investigation to get a full and complete picture of what actually took place. The employees have a strong privacy interest in their identities, which are inextricably tied to their professional and personal reputations and their roles as employees. Their privacy interest outweighs the public's interest in knowing all of the details of the investigation. Further, their involvement in an investigation that involves a potentially contentious situation may result in embarrassment or harassment. Accordingly, the staff accused in this matter as well as the individual staff members that were interviewed in the course of the investigation have substantial privacy interests in their identities.

Protecting the identities of the employees may be accomplished by redacting their names and identifying details and providing the public a redacted copy of the material. By providing a redacted copy of the information to the public, OSC would reveal general information about the investigation, thus satisfying the public interest, while protecting the employees' privacy.

This result is consistent with case law, as courts have held that serious and less serious misconduct by low-level agency employees do not have sufficient public interest to outweigh the privacy interest of the employee. *Forest Serv. Employees for Envtl. Ethics v. U.S. Forest Service*, 524 F. 3d 1021, 1025 (9th Cir. 2008). Courts have typically extended protection to the identities of mid-level and low-level federal employees accused of misconduct, as well as to the details and results of any internal investigations into such allegations of impropriety. *Stern v. F.B.I.*, 737 F.2d 84, 94 (D.C. Cir. 1984).

If you have any questions about this supplemental information or request for publication of a redacted report, please contact Sharon M. Johnston in the Office of General Counsel at 202-461-7658.

Sincerely yours,

Walter A. Hall
Assistant General Counsel

Enclosure

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

January 4, 2012

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. D1-11-2679 and D1-11-2798

Dear Ms. Lerner:

I am responding to your letter dated August 30, 2011, regarding allegations reported by an employee/Veteran, and the employee's supervisor at the Department of Veterans Affairs Boston Healthcare System (VABHS), Brockton Division (Brockton). The employee works in the business office and alleges that three other VABHS employees at Brockton improperly accessed the employee/Veteran's full medical record on several occasions, and that management failed to take appropriate action. You asked me to determine whether the information in the whistleblowers' allegations disclosed a violation of law, rule or regulation or abuse of authority.

I asked the Under Secretary for Health to review this matter and to take any actions deemed necessary under 5 U.S.C. Section 1213(d)(5). VA found that a previous privacy review, service level review, and Congressional inquiry had taken place between February 2011 and August 2011 but determined that an Administrative Investigative Board was warranted to respond to the allegations raised.

The evidence from this investigation does not substantiate the allegations that three other VABHS employees improperly accessed the employee/Veteran's full medical record or that management failed to take appropriate action. However, the investigation did find that the employee/Veteran was allowed access to her medical record while using another employee's computer access, in violation of VA policies. The investigation also found that the employee who improperly allowed access by the employee/Veteran, also improperly allowed nursing staff in urgent care to use her computer access to review electronic patient information, in further violation of VA policies. The additional findings have been referred to VABHS management for action.

The Honorable Carolyn N. Lerner

I have reviewed the report and concur with the findings, conclusions and referral for corrective action. I will closely monitor the implementation of the corrective action to ensure it is taken.

Thank you for the opportunity to respond to these issues.

Sincerely,

Eric K. Shinseki

Enclosure

(b) (6) medical record in violation of VHA Handbook 1605.2, Functional Categories Identifying Appropriate Levels of Access to Protected Health Information and if this is found to be true;

- Did management fail to take appropriate action?

2. SUMMARY OF ANY EVIDENCE OBTAINED FROM THE INVESTIGATION

A. Did (b) (6) access (b) (6) record inappropriately?

(b) (6) testified that she was assigned a project requiring her to review patient records for medical care cost recovery efforts. (b) (6) (page #8 of her testimony) verifies that she assigned this project to (b) (6). (b) (6) also verifies (on pages #33-35 of his transcript) that during his fact finding of this issue, he found (b) (6) accessed the record as part of her assigned duties and that there was no malicious intent. (b) (6) testified that she was required to print patient appointment lists and also testified that she may have accessed (b) (6) record as part of her assignment (page #5 of her transcript). (b) (6) also testified that as Administrative Officer of the Day (AOD), she is required to maintain a daily patient log for (b) (6). On page #6 of her transcript, she describes accessing patient diagnosis and other information for the daily log and gains and losses report. She testified that she never inappropriately accessed (b) (6) medical record or discussed any information gleaned from the medical record with other staff members.

B. Did (b) (6) access (b) (6) record inappropriately?

(b) (6) testified that she appropriately accessed (b) (6) medical record during her role in patient services as a (b) (6) for (b) (6). (b) (6) stated (on page #5 of her testimony) that she did access (b) (6) medical record to (b) (6) her into an (b) (6) appointment. (b) (6) states (on page #7 of her testimony) that part of her responsibility, as (b) (6) in (b) (6), was to print a patient medication list. The list was requested by nursing service for medication reconciliation purposes (this was verified by the Nurse Manager of (b) (6) as part of this investigation). (b) (6) (page #10 of her transcript) verifies that (b) (6) were responsible for printing a medication list for nursing staff. (b) (6) testified that she did not review any other part of the chart or discuss (b) (6) medical record with any other staff members. She maintains she accessed the record as part of her job responsibilities.

C. Did (b) (6) access (b) (6) record inappropriately?

(b) (6) testified that as part of her job responsibilities as (b) (6) in (b) (6), she would print patient appointment lists. This was verified by (b) (6) (b) (6) (page #10 of her transcript). On page #5 of her testimony, (b) (6) states that (b) (6) asked her to print a list of her upcoming appointments. (b) (6) (on pages #41-42 of his transcript) stated that during fact finding, (b) (6) (6) was asked by (b) (6) to review upcoming medical appointments in the

computer. On page #7 of her transcript, (b) (6) states that she was required to print medication lists for medication reconciliation for the staff in (b) (6) (this was verified by the (b) (6) Nurse Manager as part of this investigation). (b) (6) also testified that nursing staff may have used her computer access to look up other parts of the medical record while assisting patients. On pages #9-11 of her transcript, (b) (6) testified that (b) (6) asked her to review (b) (6) (b) (6) progress note so that (b) (6) could find out contents of that note. (b) (6) (b) (6) stated that she did access the note, but looked away and allowed (b) (6) to view the progress note under (b) (6) computer access. When asked directly, (b) (6) stated she never browsed (b) (6) record inappropriately.

(b) (6) states (on page #15 of her transcript) that in her opinion the employees in question acted appropriately. They did access (b) (6) medical record but did so as part of their job responsibilities.

All testimonies were consistent with the review conducted in February 2011 by the (b) (6). During his review, (b) (6) reported that she may have accessed (b) (6) record while performing her duties as AOD or when completing a billing project for (b) (6). (b) (6) reported that she may have accessed the record while performing her duties as (b) (6) in (b) (6). (b) (6) was also responsible for printing a medication reconciliation worksheet for (b) (6) staff. (b) (6) reported that she may have accessed the record while performing her duties in (b) (6) or while completing the diagnosis entry for the daily log. (b) (6) did not provide any conclusions to (b) (6); he simply reported the findings from his interviews.

D. Did management fail to take appropriate action?

During his interview, (b) (6) was asked if he was aware that (b) (6) allowed (b) (6) to review a (b) (6) progress note while using (b) (6) access. (b) (6) appeared surprised and reported he had no knowledge of this particular violation (b) (6) transcript pages #43-44). Thus, it appears Patient Services Leadership was unaware of this particular violation. The AIB also found that there was a lack of communication within the Patient Services management team and with (b) (6) regarding this matter as a whole.

3. A LISTING OF ANY VIOLATION OR APPARENT VIOLATION OF LAW, RULE OR REGULATION

Based on the interviews and additional fact finding, the AIB found that (b) (6) records were accessed by (b) (6), and (b) (6) but there was no substantiated evidence that the medical record was accessed inappropriately or maliciously and all employees accessed the record during the performance of their job.

- (b) (6), AOD (Administrative Officer of the Day), met the level based on her Functional Category: Business Office Administration in which the Conditions for Access to Information: For oversight of reimbursement, payment and financial services.

- (b) (6), (b) (6) for (b) (6) met the level based on her Functional Category: Administrative Support in which the Conditions for Access to Information: Administrative Support.

- (b) (6) in (b) (6), met the level based on her Functional Category: Administrative Support in which the Conditions for Access to Information: Administrative Support.

The AIB made two additional findings based on the testimony of (b) (6).

As testified by (b) (6), she allowed (b) (6) to review her own (b) (6) progress note while using the computer access belonging to (b) (6). This violates several VA policies, including VA Handbook 6500, Information Security Program, and VABHS' Medical Center Memorandum--00-011-LM, Information Security Program.

(b) (6) also testified that, while logged into the Computerized Patient Record System (CPRS), she allowed nursing staff in (b) (6) to review electronic patient information. This violates VA Handbook 6500, and VABHS' Medical Center Memorandum- 00-011-LM. As mandated by 38 U.S.C. § 5723(f), all VA Employees are required to read, understand and agree to abide by the National Rules of Behavior annually. The National Rules of Behavior include the following statements:

a. "I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties except as provided for in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. I also agree that I will not engage in any activities prohibited as stated in section 2c of VA Directive 6001."

b. "I will not attempt to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff."

c. "I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the VA minimum requirements for the systems that I am authorized to use and are contained in Appendix F of VA Handbook 6500."

4. A DESCRIPTION OF ANY ACTION TAKEN OR PLANNED AS A RESULT OF THE INVESTIGATION

The Facility Director approved the findings of the AIB that the two allegations were not substantiated and referred the additional findings to the Patient Services Chief for action. Appropriate action will be determined by the Patient Services Chief in consultation with the Employee Relations section of the VABHS Human Resources Service. The proposed timeline for action by VABHS is January 6, 2012.