DEPARTMENT OF VETERANS AFFAIRS
Under Secretary for Health
Washington DC 20420

OCT - 9 2015

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-14-1588

Dear Ms. Lerner:

I am responding to your request for supplemental information on the Department of Veterans Affairs (VA) investigation of allegations made by a whistleblower at the Phoenix VA Medical Center (hereafter, the Medical Center), Phoenix, Arizona. The Office of the Medical Inspector (OMI) coordinated a VA team that conducted a site visit to the Medical Center on November 3-5, 2014.

VA did not substantiate the whistleblower's three main allegations regarding supervision of surgical residents, surgeons practicing beyond the scope of their privileges, and illegal intrusions into the electronic health record (EHR) of the whistleblower.

You requested further information regarding the allegations of illegal intrusions into the EHR of the whistleblower. Specifically, you wanted further information regarding three accesses to the employee's EHR found to be authorized and in the performance of job duties in the Report. These three accesses were to obtain home address contact information to set up an entrance physical, obtain the whistleblower's work address and phone number needed for a police report, obtain contact information to get a home address to send correspondence.

In responding to your question, the original Sensitive Patient Access Report (SPAR) was reviewed again to confirm that the conclusions were supported. In doing so, we confirmed the findings and conclusion in two of the three instances.

As background, Veterans Health Information Systems and Technology Architecture (VistA) includes patient records in the Computerized Patient Record System (CPRS) module, but it is also an enterprise-wide system that includes a great deal more than just EHRs, including employee information. SPAR reports include accesses to an option that is labelled "Patient Inquiry" that should be more properly labelled Person Inquiry as it is not limited to patients. All employees (at least in VHA) have their demographic information stored here as it is a part of VistA (79VA10P2 Privacy Act system of records). So, accessing "Patient Inquiry" which would show up in a SPAR report does not mean accessing the medical record (24VA10P2 Privacy Act

system of records) which is Protected Health Information (PHI) and protected by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

The first person on the list, [redacted], was not merely accessing the EHR, he was creating it in preparation of on-boarding the whistleblower. So he would have been entering the demographic information into the record as he created it. His access was authorized.

The second, [redacted], was performing his duties as a VA police officer, accessing the demographic data in Patient Inquiry to follow up on a report of a dangerous patient. As he just used the Patient Inquiry to get demographics, the access is authorized as explained above. As the report explains (p. 19), subsequent to the time of the access by [redacted] this type of access has been limited to only the Chief of Police at each VA facility.

Review of the SPAR report shows that the third person's, [redacted] access was not to "Patient Inquiry" but was to CPRS which technically is an access to the EHR. Although the access was in performance of her official duties, and therefore, authorized under the Privacy Act, access to the EHR for employment purposes is contrary to policy and technically not authorized under the HIPAA Privacy rule. Her access would have been perfectly fine, as was [redacted] if she had accessed the exact same demographic information via "Patient Inquiry." As the report notes (pp.19, 20), remedial action has been taken to clarify and reinforce proper procedures and authorities for accessing the EHR.

Finally you asked whether these accesses comport with the Medical Center policy that states: "Medical records shall not be accessed by an employee...for the purpose of obtaining demographic information of a coworker. [emphasis added.] This includes such information as home telephone number, home address or any personal demographic information." See Policy Memorandum PO-05 June 6, 2014. The meaning of "coworker" in the policy refers to people an employee works with, rather than the records of anyone that works at the entire facility. So this policy is meant to prevent people in the same office or department from entering a record for demographic information even if to perform a valid job function, even where there would have been Privacy Act "need-to-know" and HIPAA Privacy Rule authority to access these records. In this case, these individuals are not coworkers of the whistleblower and their otherwise authorized access would not be prevented by that policy.

In summary, review of the SPAR report indicates that the conclusion at page 22, while accurate, is not complete. [redacted] access to CPRS, while not illegal or a violation of law, was technically unauthorized under the HIPAA Privacy Rule. VA's

normal procedure in such an instance is to report the access to the Privacy and Security Event Tracking System (PSETS) and have it evaluated by the VA Incident Response Team for any appropriate notification or remediation. As of this writing, the improper access via CPRS has been entered into the PSETS tracking system.

Thank you for the opportunity to respond.

Sincerely,

David J. Shulkin, M.D.