

**DI-14-1588**  
**Final Whistleblower Comments**

September 11, 2015

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

RE: OSC Case File DI-14-1588

Dear Ms. Lerner:

I have reviewed the VA OMI response entitled "DI-14-1588 Additional Information" and found it to be grossly inadequate. The response doesn't legitimately address any of the key issues I identified in my whistleblower response letters dated May 10, 2015 and July 12, 2015.

For example, the VA OMI again failed miserably to provide any logical reason as to why Dr. Deering's executive assistant Ms. Hamilton-Bell had any need to access any of my demographic data on June 28<sup>th</sup> 2013. While the VA acknowledged unauthorized medical record access occurred, the VA still contended such illegal access was essentially a harmless error that occurred while Ms. Hamilton-Bell was performing valid duties requiring access to my demographic data. However, the VA provides no legitimate evidence or statement as to why there was even a need for such demographic data access. For the reasons outlined in my previous response and reiterated in the attached document, the initial and only explanation offered by the VA is clearly fabricated to cover up one of the routine VA whistleblower retaliation technique which is unauthorized access to whistleblowers' medical records.

The VA OMI completely ignored multiple serious issues that I outlined in my initial and supplemental comments regarding the OMI report. Based on its own investigative report, the VA evidence related to attending supervision of residents showed a lack of attending physician notes/co-signatures. The OMI report also indicated strong evidence of improper nurse OR log coding. In the current "Additional Information" supplement, the VA made no attempt to reconcile these investigation findings with its illogical contention that it could not substantiate improper supervision of residents.

To date, the VA OMI has neglected to address any of my other concerns including the lack of confidentiality, failure to investigate the correct timeframe of events, Phoenix VA surgeons operating outside their scope of practice, the high number of surgical complications and related mortality, lack of appropriate facility disclosure of bad surgical outcomes, and incorrect classification of advanced laparoscopic procedures. It also failed to review the dismal ABS In-training examination scores and evaluations among surgical residents that indicate many do not

possess the surgical competency commensurate with their corresponding post-graduate residency level.

Based on the evidence and information provided in my previous whistleblower comments as well as this current document, I strongly believe the VA OMI failed to perform an earnest and unbiased investigation. By failing to adequately investigate the evidence and refusing to substantiate its conclusions, the VA OMI minimized and/or ignored the serious patient safety problems that will continue to threaten our Phoenix VAMC veterans.

Sincerely,

A solid black rectangular redaction box covering the signature area.

**1. The VA failed to give any alternative reason why Dr. Deering's administrative assistant Ms. Hamilton-Bell accessed my CPRS chart.**

Neither the VA nor Dr. Deering's administrative assistant Ms. Hamilton-Bell has given a valid explanation as to why she needed to access my demographic data in the performance of her duties on June 28, 2013. Per the reason the VA offered in its initial report, Ms. Hamilton-Bell purportedly accessed my medical record to obtain my street address in order to mail a letter to inform me of the suspension of my surgical privileges. However, the date she accessed my record was on June 28<sup>th</sup> 2013, one month after that May 28, 2013 suspension letter had been mailed to me.

As I've previously identified, the Phoenix VA employee CPRS charts list addresses and contact phone numbers that always default to the Phoenix VAMC's street address and general switchboard number. Assigning employees the Phoenix VAMC address/switchboard number automatically as the only employees' medical record demographic data has been the routine practice at the Phoenix VAMC since at least the 1980s.

As an experienced executive assistant to the Chief of Staff Dr. Deering, Ms. Hamilton-Bell would have known that no useful employee demographic data was contained in the employee's CPRS chart. Because all VA employees are required to complete the annual training on information security and privacy, she also should have been well aware that accessing an employee's medical record for demographic information is strictly prohibited.

The VA's supplemental response did not provide any alternative explanation of Ms. Hamilton-Bell's actions. The VA tried to gloss over its lack of response by stating "the access was for the performance of her official duties, and therefore authorized by the Privacy Act". The VA has given no evidence to show that she had any official duty on June 28, 2013 that required her to access my demographics in any manner at all.

Since the VA did not bother to offer any other explanation for Dr. Deering's executive assistant Ms. Hamilton-Bell access to my medical record on June 28<sup>th</sup> 2013, by default the only logical reason for her to be in my medical record is to "fish" for personal information that senior executives like Dr. Deering could use to retaliate against me.

**2. The VA inexplicably claimed that Dr. Deering's executive assistant Ms. Hamilton-Bell's access to my CPRS medical record was "not a violation of law".**

The VA tried to soften the severity of her violation by stating "Dr. Deering's executive assistant Ms. Hamilton-Bell's access to CPRS" was "not a violation of law" under the "HIPAA Privacy Rule". HIPAA is federal legislation that was passed to protect personal health information. The VA has clearly admitted that Ms. Hamilton-Bell's access to my medical record was unauthorized. By definition, unauthorized access of medical records constitutes a legal violation of both HIPAA and the Privacy Act of 1974. The VA tried to redefine federal privacy/HIPAA law as merely a "privacy rule" in order to downplay her violation. However, its feeble attempt does not change the fact that Dr. Deering's executive assistant Ms. Hamilton-Bell clearly broke federal law as well as violated numerous national VA policies on privacy and information security.

The VA stated that her access was to perform a “valid job function” but did not indicate what that function would have been on June 28, 2013. The VA further tried to dismiss the unauthorized access by implying Ms. Hamilton-Bell was not my “co-worker” and therefore did not technically violate the local Phoenix VA policy on co-workers accessing other employee’s medical charts. The national VHA directive on the VHA Privacy Program does not make any such distinctions about co-workers. This statement by the VA OMI implied that this unacceptable local HIPAA policy that was allegedly amended by the former Phoenix VA Director Sharon Helman overrides the national VA information security and privacy policies, federal HIPAA regulations, and the Privacy Act of 1974.

- 3. The VA illogically contended that the Chief of Staff’s executive assistance Ms. Hamilton-Bell would have been “perfectly fine” obtaining my information through VISTA demographics if she had chosen to do so. Likewise, the VA inexplicably contends that Officer Seibel was equally “fine” when he accessed my sensitized information.**

While not consistent with major VHA directives on privacy and information and security policies, the Phoenix VA Medical Center (VAMC) Policy PO-05 “Sensitized Patient Record Access Policy” outlines the rules of access for not only sensitized charts but also sensitized data. As per that policy, “Sensitive data includes, but is not limited to, patient identifying information such as patient name, social security number (SSN), and all health information.” Therefore, by this definition, my name, my social security number, and my health information are considered sensitive data. Because I was a VA employee, my VISTA records as well as CPRS chart were labelled as “sensitized”.

Per that policy, “All requests for sensitive information from the electronic medical record and **access to sensitized records** will be processed in accordance with the Privacy Act, Health Information Portability and Accountability Act (HIPAA), Office of Cyber and Information Security (OCIS), Information Access and Privacy OIA - Health Information Governance.” *[emphasis added]*

The VHA Privacy Program policies including information and security policies do not give employees carte blanche to access all sensitive employee data in the performance of their legitimate official duties. Each employee is obligated to access the minimum amount of data necessary to perform his or her duties.

In addition, per the 4/11/12 VHA Directive 1605 “The Privacy Policy Program” the directive requires that the VA Privacy Program have “VHA-wide compliance with all applicable privacy laws, regulations, Executive Orders and implementation policies, directives, and handbooks”. This directive requires compliance with the federal Privacy Act. As part of the VA Privacy Policy Program, the VHA Information and Security Office has interpreted privacy and information security rules to entail all employees are obligated to use the least intrusive method by which to gather information.

Overlooking the fact that neither employee had a legitimate official reason that required access to my VISTA/CPRS records, both Officer Seibel and Dr. Deering’s executive assistant Ms. Hamilton-Bell overstepped the bounds of “minimum amount of data” needed. Both had full access to my medical record, social security number and my birthday. This information was not needed for the performance of any official duties. Using the same method by which all other police officers obtain employee contact information, Officer Seibel could have obtained my contact information by simply accessing the Microsoft Outlook Global Address List, a non-sensitized source of contact information. Overlooking the

fact that there is no legitimate reason for Dr. Deering's executive assistant Ms. Hamilton-Bell to have accessed my demographic data on June 28, 2013, Ms. Hamilton-Bell could have obtained my contact information by making a simple phone call to Phoenix VAMC Human Resources. Human Resource contact is the only officially acceptable method by which all other Phoenix VA secretaries/assistants obtain employee addresses.

The VA illogically contended that the Chief of Staff's executive assistance Ms. Hamilton-Bell would have been "perfectly fine" obtaining my information through VISTA demographics if she had chosen to do so. However, as per the Privacy Act, my social security information and birthday is considered restricted and sensitive information. There was nothing in the performance of her duties that required her to access my social security number on June 28, 2013. The only legitimate way for her to obtain my address would have been to make a phone call to Human Resources.

Officer Seibel did not need to have access to my social security number or birthday in order to "follow up on a report of a dangerous patient". Overlooking the fact that the VISTA program he accessed had my sensitized data but did not list my work phone extension number or other useful contact information, Officer Seibel did not need to enter VISTA to obtain my contact information. The only way he would have had any legitimate reason to access my social security information and other sensitized data in the course of his official duties was if he was investigating me as a suspect. I clearly was not a suspect in any crime. He should have used the Microsoft Global Address List if he wanted to locate my direct contact phone number.

In addition, it was ludicrous for the VA to claim that the "Patient Inquiry" profile on VISTA menu is actually a "person inquiry" and not a "patient inquiry". That is patently untrue. That VISTA file menu was always meant to store/access patient information. Only VA Human Resource personnel have access to the "employee search" file menu keys. Officer Seibel was never assigned the file menu keys that would allow him to do an employee search. Therefore, he chose to bypass the appropriate VISTA menu security controls by searching for information on me directly through the "patient inquiry" menu which contains my restricted sensitive data. It is evident in my medical record access inquiry report that Officer Seibel has accessed "Patient Inquiry" and not "Person inquiry" as the VA wants us to believe. **(Please see Exhibit 1.)**

**4. The VA grossly neglected to address any of the legitimate concerns that I identified in my original whistleblower letter dated May 10, 2015 and follow up letter dated July 12, 2015.**

The VA OMI also completely ignored multiple serious issues that I outlined in my previous whistleblower response. Based on its previous report, the VA clearly couldn't find documentation of attending supervision of residents because there was a lack of attending physician notes/co-signatures and improper nurse coding of the OR log. In the current "Additional Information" supplement, the VA made no attempt to reconcile this lack of documentation with its illogical contention that it couldn't substantiate improper supervision of residents. It also refused to research any evidence of low resident scores on both the ABS in-training surgical residency exam report and evaluations.

The VA OMI also offered no explanation as to why it chose to violate the confidentiality of my name when I specifically requested such confidentiality for the investigation. Likewise, it didn't address why it failed to investigate the timeframes I recommended which corresponded to the most egregious patient safety violations. There was no VA comment made to explain Phoenix VA surgeons operating outside their scope of practice, the high number of surgical complications and related mortality, lack of appropriate facility disclosure of bad outcomes, or incorrect classification of advanced laparoscopic procedures.