Olare A Nelson, esq.
Attorney, Disclosure Unit OSC
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 218
Washington , D.C. 20036-4505

Re: OSC File No. DI-14-0838

Dear Ms. Nelson: March 20, 2016

On December 10,2013, during the Clinical Executive Board meeting at Northport VA, Dr. Eugene Mohan, Chief of Surgery stood and declared that his personal health information was violated and illegally accessed by multiple members of upper managment many he said, at least 5, who were present in the room.He was visibly distraught and shamed by the intrusion and he voiced his outrage and advised those in attendance a warning that their behaviors needed to stop. This and the documented inappropriate accesses to my own personal health information prompted my original discolsure to the OSC and that complaint as outlined was accepted in it's entirity for investigation.

Dr. Shulkin, in his response, is redefining what the issues are in my complaint and not addressing the draft facts. The VA has a database contaning my Personal Health Information and biometric data and other personally identified information which forms the basis of a massive system of records as a pretext for a medical record. The fact that the database is contained and shared by one exact same electronic Graphical User Interface (GUI) operating system called CPRS (Computerized Patient Record Systems) makes it inherently applicable to all the laws, regulations and rules that were cited in the draft facts of the original complaint accepted for investigation by the OSC but not limited to the privacy act of 1974 and the HIPPA act of 1996. There is no evidence that the breaches of my medical record at any time was for any legitimate or authorized purpose as it pertains to occupational health that would allow management or employees authority to access this wthout breach of the medical record.

There is rampant inappropriate access across the board at the Northport VA of medical charts and personal health information of employees and employee veterans by both management and fellow employees equating to violation of laws, rules, and regulations set forth by the U.S. government and the Veteran's Health Administration itself. This is a violation of the Privacy Act of 1974 and a violation of the HIPAA act of 1996. This is a violation of the VHA handbook series pertaining to privacy mainly 1605, 1605.1, 1605.2, 1605.03. This is a violation of VHA Handbook 6500 Information Security Program (to provide specific procedures and establish operational requirements to implement the Department of Veterans Affairs (VA) Directive 6500, Information Security Program). This is a violation of VHA Handbook 6500.2 MANAGEMENT OF DATA BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION (SPI) (This Handbook establishes procedures for Department of Veteran Affairs (VA) management of data breaches involving VA Sensitive Personal Information (SPI). It implements 38 U.S.C. §§ 5721-28; and the implementing regulations at 38 C.F.R. §§ 75.111-119, section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (codified at 42 U.S.C. § 17932) and interim final regulations at 45 C.F.R. §§ 164.400-.414, and Office of Management and Budget (OMB) Memorandum M-07-16, Safeguarding Against and Responding to Breach of Personally Identifiable Information) . This is a violation of VA Directive 6502 (the Department wide program policy for the protection of privacy of veterans, their dependents and beneficiaries, as well as the privacy of all employees and contractors of the Department of Veterans Affairs (VA), and other individuals for whom

personal records are created and maintained in accordance with Federal law. This directive clarifies policies, roles, and responsibilities for the VA Privacy Service, also known as the VA Enterprise Privacy Program, the program that oversees all VA-wide privacy programs). This is a violation of VA Handbook 6502.1 (This handbook revises Department-wide procedures for the OneVA tracking of complaints and privacy incidents, and implements the policies set forth in Department of Veterans Affairs (VA) Directive 6502, VA Enterprise Privacy Program, and VA Handbook 6500.2, Management of Security and Privacy Incidents). This is a violation of the Federal Standards for Privacy of Individually Identifiable Health Information (IIHI) and/or the Security Standards for the Protection of Electronic Protected Health Information (PHI) (45 CFR Parts 160 and 164, Subparts A, C & E, the Privacy and Security Rules and the Breach Notification Rule Subpart D - Notification in Case of Breach of Unsecured Protected Health Information) (45 CFR SS 164.400 - 164-414).

The multiple accesses to my VA medical records in all the instances were **not** for treatment, payment or healthcare operations. I was never a patient nor did I ever seek pre-employment , employment physicals or any other care from Employee Health Services. Furthermore I **never** sought healthcare on any of the dates/times of many the entries in the SPAR so the access was **not** necessarily related to any need for occupational health, employee health to review or enter any data for any employment purpose such as functional statements (FS), job title, role, etc. This is therefore a continued violation of law, rule and regulation as detailed above.

This outrageous vulnerability and breach of medical record information on the part of both employees and management not only equates to violaton of the above privacy laws, it is serves a a distinct percieved and accepted deterent for multiple employees who are veterans to seek their needed care. Dr. Shulkin's response limits it's scope and underscores the real harm here for veterans and my primary motivating factor in becoming a whistleblower. As a physician, my knowledge of the vulnerability and the documented inappropriate access of medical records violates rules of law and the physician–patient relationship. The fact that this occurs in the VA and employee veterans know this, this is a HUGE obstruction for them to access care. How can a veteran who is entitled and wants to use the VA do so knowing that the risk of their supervisors and fellow employees can read their medical information? How can these breaches and documented access be dismissed by the VA ? I have witnessed my own veteran colleagues and many of them my own patients, be vilified and humiliated by breaches of their medical record. Employee health records are not even visible to anyone other than employee health personnel. Therefore, those who enter the medical record, who are not the employee health clinician, especially management officials, do so not to review employee health records because they can't; (management knows the occupational and employee health records are not viewable) nor do they review for fitness for duty BUT to look at their personal medical chart aka PHI. Employers should NOT have this right nor should they be excused for culpability here because to do so fosters a culture of intimidation and vulnerability for our veteran employees and all the non-veteran employees. This is a violation of the laws cited above and the VA response equates to a whitewash and ignores the facts.

Additionally, half of my original complaint was that I was witness to the Northport VA Chief of Surgery's declarartion in a public forum, that his medical record was breached not once, not accidentally ,but, according to him knowingly and inappropriately by senior individuals in management multiple times. This was never investigated nor was the OMI investigation and interviews willing to even engage in recorded or sworn testimonies to investigate this. I am not privy if Dr. Eugene Mohan cited in my original complaint filed his own complaint, but ,even if he didn't it does not mean it should not be investigated. This was an accepted part of the OSC original complaint and ignored by the agency's investgative body, the OMI and ignored in its response. If we witness someone declare violation of the

law and perform no investigation, how is that acceptable? Is it acceptable if you choose to do an investigation and it is conducted in an inadequate way with an underlying dissmissive attitude as I expressed to you in my prior letters? If you investigate appropriately and find no evidence, that is legitimate. But how can the OMI's report and findings have any legitimacy when as cited in my prior letters, they refused to conduct a proper investigation. The testimonies were not sworn nor where they recorded. Thus, the VA's self serving conclusions cannot be independently authenticated.

The accessibility and breaches of privacy breach the medical ethical priniciples of non-malefescence, beneficence, and justice that must exist between patient and physician without which the therapeutic relationship suffers. These ethical principles do not exist solely when procedures are performed or medications are prescribed, they exist in all aspects of the relationship and very often the most significant vulnerability and harm to a patient is breach in their personal health information. The harm is that the patient who seeks care does so with the understanding that what is discussed and/or recorded between physician and patient is maintained in confidence. At no time is there disclosure made to the patient employee or veteran employee who is a patient that their personal Health information is accesible and allowed to be viewed by management even in the instances Dr. Shulkin claims exemption: "It is not correct that employees should not access another employees medical record even though the later employee is not a Veteran receiving medical care at the facility." In each instance when there is a potential risk of PHI to be shared, we obtain informed consent or provide a signed release. There is no informed consent here, nor is there a signed release and there should be by the individual employee and the employee veteran.

Employee veterans should be advised their PHI is accessible by their supervisors, fellow employees prior to engaging in care because to continue to do this without that consent, ignores a real and significant risk to employee veteran patients. According to the VA TMS, Talent Management Systems, the mandatory training annually for all employees on patient abuse pp6 and 13, it is clearly stated there that privacy breaches are a form of patient abuse. Yet, the VA continues to handle these breaches as a knowledge deficit instead of the potentially criminal act it is. It violates the principle of nonmalefescence. This undermines patient care services we provide to veterans and undermines the Veterans Preference Act for hiring. A veteran who seeks employment at the VA is afraid to be hired because at the same time his/her access to care at the VA is threatened as a result of this distinct risk of a privacy breach.

Despite the physician's intent for benefiscence in delivering care in a setting to preserve their patient's confidence, the access from managers as well as employees, again breaches that. These breaches have violated the laws and serve s a deterrent and interference to employee veterans seeking care. This equates to a roadblock for veteran employee's access to care. I know first hand, that after the Clinical Executive Board meeting as Surgery Chief's treating physician, Dr. Susan Stickevers revealed she needed to maintian a separate and distinct medical record to thwart senior management from continued access to his chart. She was never interviewed. Repeat offenders are especially problematic and stating that they had a continued ongoing knowledge deficit is really a poor excuse especially if those individuals are in management. They can easily be identified with a review of all the data accumulated by both th OMI and the OSC and those repeat offenders should be identified with proper investigation.

There is currently a distinct disadvantage for a veteran employee patient regarding their PHI vs. private sector counterparts because the VA as their employer also happens to be the maintainer of their medical records with their massive Systems of Records (SOR). The VA SOR contains very detailed

biometric data, Protected Health Information (PHI), Sensitive Protected Information (SPI), Personally Identifiable Information (PII), Individually Identifiable Information (III) and Individually Identifiable Health (IIHI) Information that can be easily accessed by any VA employee. All employee veterans deserve the same privacy rights non –veteran employees have in the community and to have an environment of care that consists of privacy breaches for the employee veteran and the employee of the VA, equates to violating the principle of Justice that mandates all patients regardless of their status, receive equal care. Employee veterans need to be treated with the same standards as non-employee veterans and not to do so violates the principle of justice for which the VA as a preferential employer by law of veterans has a unique, undeniable and higher responsibility to assure this is not breached. The VA has failed to uphold biomedical ethical principles for which some of the above laws cited eminate from. This needs to stop and those who have been shown to have inappropriately accessed patient records have violated the laws outlined above and ought to be accountable.

Thank you for the opportunity to provide a response.

Sincerely,

Athena Zias Dilena, MD