DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

October 20, 2016

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-15-0971

Dear Ms. Lerner:

I am responding to your letter regarding allegations made by a whistleblower at the Northport Department of Veterans Affairs (VA) Medical Center (hereafter, the Medical Center), Northport, New York. The whistleblower made allegations of 829 intrusions into his electronic health record and of violations of his privacy by the 119 individuals who made those intrusions, maintaining that these actions may constitute violations of law, rules or regulations, and gross mismanagement, which may lead to a substantial and specific danger to public health. 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 Under Secretary for Health directed the Office of the Medical Inspector to assemble and lead a VA team to conduct an investigation. The report substantiates both allegations and makes two recommendations to the Medical Center.

Thank you for the opportunity to respond.

Sincerely,

Robert D. Snyder
Chief of Staff

Enclosure

DEPARTMENT OF VETERANS AFFAIRS
Washington, DC

Report to the
Office of Special Counsel
OSC File Number DI-15-0971

Department of Veterans Affairs (VA)
Northport VA Medical Center
Northport, New York

Report Date: September 27, 2016

TRIM 2015-D-6693

Executive Summary

The Under Secretary for Health (USH) directed the Office of the Medical Inspector (OMI) to investigate allegations lodged with the Office of Special Counsel (OSC) concerning the Northport Department of Veterans Affairs (VA) Medical Center (hereafter, the Medical Center), located in Northport, New York. [redacted] (the whistleblower) alleged that employees there are engaging in conduct that may constitute violations of laws, rules or regulations, and gross mismanagement, which may lead to a substantial and specific danger to public health. The VA investigative team conducted site visits to the Medical Center on March 21–24 and August 23–25, 2016.

Allegations

Specifically, the whistleblower alleged that:

1. Beginning in October 2007, Northport VAMC employees have repeatedly accessed his medical record for unknown reasons and without cause; and

2. This improper access of his medical records constitutes an impermissible intrusion into his privacy and is a violation of law and agency policy.

VA **substantiated allegations** when the facts and findings supported that the alleged events or actions took place and **did not substantiate allegations** when the facts and findings showed the allegations were unfounded. VA was **not able to substantiate allegations** when the available evidence was not sufficient to support conclusions with reasonable certainty about whether the alleged event or action took place.

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

Conclusions

- VA **substantiated** that 48 of the 829 (6 percent) instances of access to the whistleblower's electronic health record (EHR) between October 17, 2007, and December 1, 2014, were improper. In 47 of these instances, we could find no reason for the accesses. In the last instance, we believe the access was improper but performed in error. We further **substantiated** that these improper accesses may have violated the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.
- By January 13, 2014, the Medical Center had completed an enhanced training program to reduce improper accesses of the EHR by their employees. VA **substantiated** that 1 of 326 (0.3 percent) instances of access to the whistleblower's EHR between January 14, 2014, and December 1, 2014, the period of time after completion of the enhanced training program, was improper. VA **substantiated** that 47 of 503 (9 percent) instances of access to the whistleblower's EHR between

October 17, 2007, and January 14, 2014, the period of time before completion of the enhanced training program, were improper. At least as evidenced by this one Veteran's case, we conclude that the Medical Center's efforts to reduce improper accesses of the EHR have been dramatically successful.

Recommendations

The Medical Center:

1. Report the 48 instances of improper access of the whistleblower's EHR to the Privacy and Security Events Tracking System (PSETS). Pursuant to VA Breach Policy (VA Handbook 6500.2, *Management of Security and Privacy Incidents*), the facility Privacy Office makes this report, and once these improper accesses have been reported to PSETS, the VA Data Breach Resolution Service (DBRS) determines whether each improper access is a breach, as defined by the HIPAA Breach Notification Rule. If the improper access is determined to be a breach, DBRS will report it to the Department of Health and Human Services, per policy, and recommend notifying the affected employee.

2. Take appropriate action regarding those employees who improperly accessed the whistleblower's EHR.

Summary Statement

VA has developed this report in consultation with Veterans Health Administration (VHA) and VA offices to address OSC's concerns that the Medical Center may have violated law, rule or regulation, engaged in gross mismanagement and abuse of authority, or created a substantial and specific danger to public health and safety. In particular, the Office of General Counsel has provided a legal review, and the Office of Accountability Review has reviewed the report and has or will address potential senior leadership accountability. Our investigation revealed 47 instances where we could not confirm that there was legal authority under the Privacy Act of 1974 or HIPAA Privacy Rule for access to the whistleblower's EHR.

Table of Contents

I. Introduction

The Under Secretary for Health (USH) requested that the Office of the Medical Inspector (OMI) investigate an allegation of improper accesses of an employee's electronic health record (EHR) at the Northport Department of Veterans Affairs (VA) Medical Center (the Medical Center), located in Northport, New York. Specifically, [redacted] (the whistleblower), a patient and employee at the Medical Center, lodged a complaint with the Office of Special Counsel (OSC) alleging that other Medical Center employees accessed his EHR for unknown reasons and without cause. The whistleblower also alleged that these employees engaged in conduct that may constitute a violation of law, rule, or regulation, and an abuse of authority.

II. Facility Profile

The Medical Center, part of Veterans Integrated Service Network (VISN) 3, provides comprehensive primary care, tertiary care, and long-term care, including medicine, surgery, psychiatry, physical medicine and rehabilitation, neurology, oncology, dentistry, and geriatrics. The Medical Center consists of an acute care hospital, an extended care facility, an outpatient pavilion, Community-Based Outpatient Clinics (East Meadow, Patchogue, and Riverhead, New York), and three mental health satellite clinics (Islip, Lindenhurst, and Valley Stream, New York). The Medical Center operates 293 beds with 35 medical-surgical beds, and a 9-bed Emergency Department (ED) with one surgical treatment room. In addition, it operates 170 long-term care beds spread over four Community Living Centers. The Medical Center is a tertiary care facility that supports education and research, is affiliated with the State University of New York Medical School at Stony Brook among other academic institutions, and annually trains over 100 university residents, interns, and students. Some 34,700 unique patients are seen per year, with 4,000 inpatient admissions and over 370,000 outpatient visits.

III. Allegations

Specifically, the whistleblower alleged that:

1. Beginning in October 2007, Northport VAMC employees have repeatedly accessed his medical record for unknown reasons and without cause; and

2. This improper access of his medical records constitutes an impermissible intrusion into his privacy and is a violation of law and agency policy.

IV. Conduct of Investigation

The VA investigative team (VA team) consisted of [redacted], M.D., Deputy Medical Inspector for National Assessments; [redacted] RN, MSN, Clinical Program Manager; [redacted], Ph.D., Statistician, all of OMI; and [redacted], JD, RHIA, Director, Veterans Health Administration (VHA) Information Access and Privacy Office. The VA team reviewed portions of the whistleblower's EHR and relevant policies,

procedures, reports, memorandums, and other documents, a full list of which is in Attachment A.

On December 1, 2015, the VA team interviewed the whistleblower by telephone. Based on that conversation, we clarified the list of EHR accesses and EHR accessing individuals provided in the Special Counsel's letter to the Secretary. In an email dated February 10, 2016, OSC and the whistleblower agreed on this clarified list of accesses and accessing individuals that would be the subject of this investigation. The full list of accesses and individuals is in Attachment B, arranged from most recent access to the most remote one. The columns of the list give the name of the accessing employee, the date and time of the access, the accessing option by which the employee accessed the whistleblower's EHR in the truncated form in which it appears on the whistleblower's Sensitive Patient Access Report ((SPAR) see below for a detailed description of this report), the fully spelled-out title of the accessing option that corresponds to the truncated form, and the unique number we assigned to each access for the purpose of this investigation.

We conducted a site visit to the Medical Center March 21−24, 2016. On March 21, we held the entrance briefing with the Chief of Staff (CoS), Associate Director of Patient Care Services, and the Assistant to the Medical Center Director. On March 24, we conducted a face-to-face interview with the whistleblower. All the other individuals we interviewed are listed by name and position in Attachment C. We held an exit briefing which included the Medical Center Director, Associate Director, CoS, Associate Director of Patient Care Services, and the Assistant to the Medical Center Director on March 24.

We conducted a second site visit August 23−25, 2016. On August 23, we held the entrance briefing with the CoS, the Associate Director, and the Assistant to the Medical Center Director. The individuals interviewed are listed by name and position in Attachment C. We held the exit briefing with the Medical Center Director, the CoS, the Associate Director, and the Assistant to the Medical Center Director on August 25.

On September 14, 2016, we also conducted telephone interviews with additional Medical Center employess listed in Attachment C.

VA **substantiated** allegations when the facts and findings supported that the alleged events or actions took place. VA **did not substantiate** allegations when the facts showed the allegations were unfounded. VA **was not able to substantiate** the allegations when there was no conclusive evidence to either sustain or refute the allegation.

V. Background

The Privacy Act of 1974, 5 United States Code § 552a, prohibits agencies from disclosing any record contained in a system of records except with prior written consent

of the individual to whom the record pertains, unless permitted under a statutory exception. In particular, § 552a(b)(1) allows for disclosure to officers and employees of the agency maintaining the record in performance of their duties. This is often referred to as an employee's "need to know."

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 Code of Federal Regulations (CFR) Parts 160 and 164, requires that covered entities, including VHA, "ensure the confidentiality. . . .of all electronic protected health information [PHI] the covered entity. . . .maintains." The Breach Notification Rule requires patient notification for certain incidents involving access to or disclosure of PHI in a manner not permitted under the Privacy Rule.

Under the HIPAA Privacy Rule, a covered entity such as VHA may use or disclose PHI only as specifically authorized by the regulation and as required by law. Specifically, the HIPAA Privacy Rule permits a covered entity to use and disclose PHI as provided in 45 CFR § 164.502. Although the definition of PHI excludes health information in "employment records held by a covered entity in its role as employer," the term encompasses "individually identifiable health information" created, received, or maintained by a covered entity in its health care capacity, including health information of a covered entity's employee (45 CFR § 160.103; 67 Fed. Reg. 53182, 53192, Aug. 14, 2002). To that end, the Department of Health and Human Services (HHS) has stated that:

> It does not matter if the individual is a member of the covered entity's workforce or not. Thus, the medical record of a hospital employee who is receiving treatment at the hospital is protected health information and is covered by the Rule, just as the medical record of any other patient of that hospital is protected health information and covered by the Rule.

As with any PHI, a covered entity may not use or disclose PHI of an employee without a HIPAA exception, such as treatment, payment or health care operations, and in most cases will need the employee's authorization to access or use the medical information for employment purposes.

VHA Handbook 1605.02, *Minimum Necessary Standard for Protected Health Information*, provides mandatory guidelines for the use and disclosure of patients' individually-identifiable health information. It explains that VHA constitutes a covered entity, and as such, is required to implement the "minimum necessary standard." This standard requires covered entities to establish policies to limit the use or disclosure of PHI to the minimum amount necessary. To accomplish the goal of limiting the use of PHI, the Handbook divides employees into functional categories, each with an appropriate level of minimum access. Individuals in administrative support positions, as outlined in Appendix B of the Handbook, have limited access to medical records when necessary to complete an assignment. The Handbook, paragraph 6, specifically states that all VHA personnel must use no more PHI than is necessary to perform their specific job function and must not access information that

exceeds the limits of their functional category. Paragraph 6 further notes that, even if an employee's position allows for greater access, the employee should only access the information necessary to perform an official function.

The VA Electronic Health Record

VHA's system of records includes the EHR, which is comprised of a graphic user interface (GUI), the Computerized Patient Record System (CPRS) displaying the Veterans Health Information Systems and Technology Architecture (VistA), a health information technology (IT) system built on a client-server architecture that ties together workstations and personal computers with GUIs, such as CPRS, and includes links allowing commercial off-the-shelf software and products to be used with existing systems. CPRS is a VHA-wide application between VistA and users that supports all clinical and administrative functions, allowing clinicians, support staff, and others access to the EHR. CPRS allows the user to enter, review, and continuously update patient information. It also supports the practitioner's review and analysis of patient data to permit clinical decision making. Access to VistA and CPRS is restricted according to the user's official information requirement.

The Sensitive Patient Access Report

SPAR documents users' access to the EHR of a patient or employee whose record is defined as sensitive. Before a user can enter a sensitive record, he or she encounters a warning that the record is sensitive, access to it is tracked, and he or she must be able to prove a need to know. The user must acknowledge this warning before access to the sensitive record is allowed, and the EHRs of Veterans who are also VA employees are "sensitive" by definition. SPAR provides a definitive list of users who have accessed a sensitive record, as well as the software path through which they accessed that record. The software paths relevant to this investigation are defined in Attachment D.

Access Criteria and Information Collected for Each EHR Access

We assessed each employee's access to the whistleblower's EHR and determined whether it was **proper** or **improper**.

We define **proper** access as one that was either documented by a provider note or an electronic signature in the EHR at the date and time of the access, or one in which there was no progress note, but the EHR or the consistent testimony of interviewees showed evidence of an authorized activity by the person who accessed the record. For example, a staff member who was responsible for inviting patients to an annual event held for the patients may have properly accessed a patient's EHR to obtain contact information like a telephone number or mailing address. However, the individual performing this task would not explicitly sign the patient's EHR. In such an instance where the staff member accessed the whistleblower's EHR on a date when such EHR access would be expected to occur, and with the testimony of other staff members corroborating that inviting patients to this event was part of this staff member's duties,

VA concluded it was more likely than not that the access was in support of the patient-related activity, and therefore, proper.

We defined **improper** access as falling into one of the following three subcategories:

- **Mistaken access:** The user mistakenly accessed the whistleblower's EHR, while attempting to access another Veteran's record. In this instance, the second patient's last name or identifying information (the first letter of the last name along with the last four digits of the social security number) was identical or very similar to that of the whistleblower. Although VA believes this subcategory of error to be an honest one, the employee did not have an official reason to be in the whistleblower's record, and therefore, the access was improper.
- **Access for no apparent reason:** VA was unable to find any documentation in the EHR or consistent testimony supporting the need for access. Without evidence of an official reason for access, VA concludes that the minimum necessary standard was not met and access was improper.
- **Access for an unauthorized reason:** VA found evidence that access was not permitted under the Privacy Act or the HIPAA Privacy Rule, and therefore, was improper.

VA obtained the following information on each employee who accessed the whistleblower's EHR, and then made a determination as to whether the access was proper or improper:

- Name,
- Title at the time of the alleged instance of improper access,
- Name and title of supervisor,
- Date and time of alleged improper access,
- Main job responsibilities around the time of alleged improper access (this section gives the general reason the employee would be in any EHR); and
- Reason employee entered the whistleblower's EHR (this section gives the specific reason the employee entered the whistleblower's record on the date and time indicated in the SPAR).

The determination of the appropriateness of each employee's access of the whistleblower's EHR is listed in Attachment E.

VI. Findings

The Medical Center conducted a comprehensive review of their practices to safeguard the PHI in the EHR based on the recommendations of four previous VA reports.[1]

[1] These reports are OSC File No. DI-13-3661, October 3, 2013, with a supplemental report on April 25, 2014; OSC File No. DI-14-0062, January 31, 2014, with supplemental reports on June 25, 2014, July 17, 2015, and July 29, 2016; OSC File Nos. DI-14-0838 and DI-14-1959 with a supplemental report on December 3, 2015; and OSC File No. DI-14-5178, May 11, 2015.

Based on this reveiw, the Medical Center conducted a mandatory 15-minute training session for all Medical Center employees, emphasizing the importance of accessing the EHR only when there is an authorized need. The initial training was completed on January 13, 2014, and sustainment training with the same content was incorporated into the training of new employees at the start of their employment. Because of this remedial action, we report our findings on or before January 13, 2014, compared with after that date, as well as the overall findings.

We investigated 829 accesses by 119 employees occurring between October 17, 2007, and December 1, 2014. Overall, we found that 781 (94 percent) accesses were proper and 48 (6 percent) were improper. In 105 of the 119 employees (88 percent), we found only proper accesses; in the other 14 employees, we found between 1 and 14 improper accesses. Of the 14 employees for whom we found improper accesses, the Medical Center reports that 6 are still employed there while 8 are not.

We found that 503 accesses (61 percent) occurred on or before January 13, 2014, while 326 accesses (39 percent) occurred after that date. In the group of accesses on or before January 13, 2014, we found 47 improper accesses (9 percent) while in the group of accesses after January 13, 2014, we found a single improper access (0.3 percent) which we determined was a mistaken access.

In 47 of the improper accesses, we found no reason to explain the accesses in our review of the whistleblower's EHR, other Medical Center records or through our interviews with supervisors and employees. Specifically, in these accesses, we could not determine that the employee accessed the EHR for treatment, payment, or health care operations or to conduct their official duties. However, in each of these 47 improper accesses, we could not be certain that a need did not exist. In the additional one improper access, we found evidence of a mistaken access.

With regard to the HIPAA Breach Notification Rule, we found no evidence that the single mistaken access was intentional, made in bad faith, outside the scope of the individual's authority or resulted in further disclosure of the information. In the remaining 47 accesses for which we found no apparent reason for the accesses, while it does not appear they were malicious or resulted in any further use or disclosure of information, they were intentional and may have been outside the scope of the individual's authority.

VII. Conclusions

- VA **substantiated** that 48 of the 829 (6 percent) instances of access to the whistleblower's electronic health record (EHR) between October 17, 2007, and December 1, 2014, were improper. In 47 of these instances, we could find no reason for the accesses. In the last instance, we believe the access was improper but performed in error. We further **substantiated** that these improper accesses may have violated the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

- By January 13, 2014, the Medical Center had completed an enhanced training program to reduce improper accesses of the EHR by their employees. VA **substantiated** that 1 of 326 (0.3 percent) instances of access to the whistleblower's EHR between January 14, 2014, and December 1, 2014, the period of time after completion of the enhanced training program, was improper. VA **substantiated** that 47 of 503 (9 percent) instances of access to the whistleblower's EHR between October 17, 2007, and January 14, 2014, the period of time before completion of the enhanced training program, were improper. At least as evidenced by this one Veteran's case, we conclude that the Medical Center's efforts to reduce improper accesses of the EHR have been dramatically successful.

VIII. Recommendations to the Medical Center

1. Report the 48 instances of improper access of the whistleblower's EHR to the Privacy and Security Events Tracking System (PSETS). Pursuant to VA Breach Policy (VA Handbook 6500.2, *Management of Security and Privacy Incidents*), the facility Privacy Office makes this report, and once these improper accesses have been reported to PSETS, the VA Data Breach Resolution Service (DBRS) determines whether each improper access is a breach as defined by the HIPAA Breach Notification Rule. If the improper access is determined to be a breach, DBRS will report it to HHS, per policy, and recommend notifying the affected employee.

2. Take appropriate action regarding those employees who improperly accessed the whistleblower's EHR.

IX. Summary Statement

VA has developed this report in consultation with VHA and VA offices to address OSC's concerns that the Medical Center may have violated law, rule or regulation, engaged in gross mismanagement and abuse of authority, or created a substantial and specific danger to public health and safety. In particular, the Office of General Counsel has provided a legal review, and the Office of Accountability Review has reviewed the report and has or will address potential senior leadership accountability. Our investigation revealed 47 instances where we could not confirm that there was legal authority under the Privacy Act of 1974 or HIPAA Privacy Rule for access to the whistleblower's EHR.