2012-02359-IQ-0092

Memorandum to the File
Case Closure

Alleged Fraudulent My HealtheVet Activity
VA Hudson Valley Health Care System, Montrose, NY
(2012-02359-IQ-0092)

VA Office of Inspector General Administrative Investigations Division investigated an allegation that VA Hudson Valley Health Care System (HVHCS) management forced employees to create fraudulent My HealtheVet (MHV) accounts and forged the MHV authentication process without veterans' knowledge. To assess the allegation, we interviewed Mr. [redacted]; Dr. [redacted] VA employees, and; a former VA employee. We also reviewed email records, Federal laws, regulations, VA and local policy, and other relevant documents. We investigated another allegation, which we discuss in another memorandum, and we will not discuss it further in this memorandum.

Standards of Ethical Conduct for Employees of the Executive Branch state that an employee shall put forth honest effort in the performance of their duties. It also states that employees shall disclose waste, fraud, abuse, and corruption to appropriate authorities. 5 CFR §§ 2635.101(b)(5) and (11). VA policy requires annual security awareness training for users of VA information systems or VA sensitive information and that users of VA information systems are responsible for signing an acknowledgment that they read, understood, and agreed to abide by the VA National Rules of Behavior on an annual basis. VA Directive 6500, Paragraph 4g, (September 20, 2012). VA policy defines unauthorized access as gaining logical or physical access to VA information or information systems either without authorization or in excess of previously authorized access and VA sensitive information/data as all Department information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. VA Handbook 6500, Appendix A, Paragraphs 72 and 76, (September 20, 2012). Further, supervisors must analyze the duties performed by their employees to ensure separation of duties and verify that users only have the system privileges that are needed to perform their assigned duties, and the Information Security Officer (ISO) will monitor compliance with separation of duties and confirm appropriate actions taken to correct any conflicts. This type of control must ensure that a single individual cannot subvert a critical process. Id., at Appendix F, Paragraph 2a, Section (5)i.

Background

MHV exists as an online personal health record that allows veterans to become informed partners in their healthcare. To access their health record online, veterans must first register online, using a computer, at www.myhealth.va.gov. To view key portions of their VA health record and use Secure Messaging (SM), a web-based encrypted communication between patients and healthcare pratitioners, veterans are required to receive VA healthcare services, register on MHV as a VA patient, and

possess an upgraded account. In order to use SM, a veteran is presented with the terms for using it and chooses to "Opt-In", which confirms that the veteran agrees to the terms of use for SM. To get an upgraded account, the veteran's identity must be authenticated by VA before allowing access to their VA health record online. The two ways to upgrade an MHV account is through in-person or on-line authentication. This verification is a one-time process that allows a veterans to upgrade their MHV account to increase access to current and future available electronic health record information and establishment of a MHV personal health record. The process verifies a veteran's identity, while ensuring security of Personal Identifying information. A veteran completes the process by visiting their local VA healthcare facility and by following these steps:

- Complete and sign VA's Release of Information form 10-5345a-MHV
- Visit a local VA facility and present a government-issued photo
- After VA staff verifies the Veteran's information, the MHV account can be upgraded for online access

Before a veteran upgraded their MHV account on-line, the veteran needed to:

- Register as a VA patient in MHV
- Have eBenefits/DS Logon Premium account
- Have MHV account information match DEERS information

Alleged MHV Fraudulent Activity

Mr. [redacted] and Dr. [redacted] told us that they never forced VA employees to, or themselves, create fraudulent MHV accounts or forge the MHV verification process. They said that they had no knowledge of any VA employee creating fraudulent accounts or forging the MHV verification process.

Records of a factfinding conducted by Dr. [redacted], in April 2012, as the result of an anonymous telephone call to Mr. [redacted], reflected that MHV technicians allegedly tried to "opt-in" veterans without their knowledge. Dr. [redacted] told us that the [redacted] instructed him to conduct a factfinding inquiry and that his inquiry revealed no misuse or problems with the HVHCS MHV system. Dr. [redacted] concurred with the factfinding report, sigining it on April 18, 2012. Meeting notes, dated April 19, 2012, HVHCS staff discussed discussed Dr. [redacted] findings and recommendations. The notes reflected that all the technicians said that Mr. [redacted] trained them on the proper "opt-in" procedures and disclosed that management observed technicians, finding no deviations from proper process protocol. Mr. [redacted] told us that following the April 2012 fact-finding, HVHCS conducted meetings, reminders, and retraining for the staff.

Dr. [redacted] told us that during his factfinding effort, two VA employees reported "rumors" that VA employees signed-up veterans without the veteran being present. Mr. [redacted], told us that through hearsay he learned that some of the

technicians performed all three MHV steps at once. Mr. [redacted] said that he thought the three-step process made it too easy to perform fraudulent activity; however, he had no knowledge that such occurred. Ms. [redacted], told us that she heard that Ms. [redacted], told Ms. [redacted], and Ms. [redacted] to auto enroll veterans into MHV without the veterans being present; however, Ms. [redacted] told us that she never told anyone to auto enroll veterans. Ms. [redacted] told us that she did not recall Ms. [redacted] instructing, condoning, or using the term auto enroll, and Ms. [redacted] told us that Ms. [redacted] never asked her to auto enroll veterans. Eleven other VA employees and one former VA employee told us that they held an in-depth understanding of the MHV program and that none of the individuals had any evidence that VA personnel forced employees to create MHV accounts or go through the authentication process without a veteran's knowledge or approval.

MHV Quota System

Although we found no evidence of VA employees creating fraudulent MHV accounts or forging the MHV authentication process, we found that some employees discussed the MHV quota system as reflected in the following emails:

- In a November 14, 2011, email, [redacted], said that VA's Secretary challenged each VISN to enroll 50% of its unique veterans in virtual health (Telehealth or MHV/Secure Messaging) by the end of FY14, with 15% expected to enroll by the end of FY12, and 30% by the end of FY13.

- In a February 3, 2012, email, Mr. [redacted] said that MHV became a major national initiative from Central Office and that VA's Secretary set aggressive goals for the next 3 years. He said that by the end of FY14, VA would have 50% of its veterans enrolled in some form of virtual healthcare and that in order to achieve these goals, it was important that all staff members become familiar with MHV and the advantages it offers.

Ms. [redacted] told us that the quota system took the human element out of healthcare, and it made it more like going to the bank or buying a car. She said, "The management of this program, regarding My HealtheVet, is unrealistic, and is making people feel, as well as the veteran, uncomfortable, and it's not conducive to a voluntary program to have these quotas met."

MHV Protective Measures

Ms. [redacted], told us that measures existed to prevent VA employees from creating MHV accounts without the veterans' knowledge but that all MHV Coordinators received face-to-face education from VA's Privacy and Health Information Management representatives, on

monthly MHV Coordinator calls, as well as taking VA mandatory privacy and security training.

Network Security Operations Center (NSOC)

NSOC records reflected instances when VA staff did not adhere to MHV protective measures. For example in one, dated July 23, 2012, a VHA Issue Brief and a VA NSOC ticket #0577333, reflected that six VA sites to include HVHCS experienced staff improperly accessing and/or taking actions in veterans' MHV accounts. The six VA sites involved were Northport, NY, Martinsburg, WV, Washington DC, West Haven, CT, Cleveland, OH, and Hudson Valley, NY. The Austin Information Technology Center and NSOC received notification about these facilities and MHV activities, and they followed up on all with appropriate action, as cited below:

- Retrain MHV staff in privacy procedures
- Administrative access deactivated
- Employees identified and told to cease inappropriate process
- Management working on implementing disciplinary action
- Privacy Officers involved
- MHV policy workgroup finalizing a list of recommendations to improve MHV privacy and security posture
- Rules of Behavior specific to MHV
- Director issued Memorandum to veterans that disclosed unusual MHV account activity

There were also instances in which veterans claimed that someone unknown accessed their account; however, these were unfounded. Ms. [redacted], told us that in one instance HVHCS received notification on July 27, 2012, that a veteran claimed that their MHV password changed without their request. However, Mr. [redacted] told her that the MHV authenticators did not have access to the passwords or to the answers to the challenge questions, so they could not have changed it. Ms. [redacted] said that in this instance, she and Mr. [redacted] drafted and disseminated a memo reiterating the registration and verification process. In another instance, Ms. [redacted], told us that another veteran reported that they did not "opt-in" for SM, but Ms. [redacted] said that the MHV account identified was not directly affected, since the MHV authenticators could not access the veteran's account.

Conclusion

We did not substantiate that HVHCS management forced employees to create fraudulent MHV accounts or forge the MHV authentication process without a veteran's knowledge or authorization. Although some employees expressed a concern about the MHV quota system, we found no evidence that it created any fraudulent activity. We found that other VA facilities experienced staff improperly accessing and/or taking actions in veteran's MHV accounts; however, we found that corrective actions were taken to address those matters. We are therefore closing this allegation without a formal report or memorandum.

Prepared [redacted] 9/3/2013
Date

Approved By: [redacted] 9/3/13
Date