DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Healthcare Inspections

VETERANS HEALTH ADMINISTRATION

Episodes of Non-Adherence to Privacy and Security Policies at the Tibor Rubin VA Medical Center

Long Beach, California

HEALTHCARE INSPECTION

REPORT #17-03557-177

JULY 31, 2019

The mission of the Office of Inspector General is to serve veterans and the public by conducting effective oversight of the programs and operations of the Department of Veterans Affairs through independent audits, inspections, reviews, and investigations.

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

The VA Office of Inspector General (OIG) conducted a healthcare inspection in response to episodes of non-adherence to Veterans Health Administration (VHA) and VA policies on patient information privacy and security identified during an unrelated OIG investigation at the Tibor Rubin VA Medical Center (facility), Long Beach, California.

Specifically, the issues were the

- Lack of software interface between VHA medical devices and the electronic health record (EHR), and inappropriate staff workarounds,[1]
- Lack of biomedical engineering (Biomed) and information technology (IT) assistance in resolving software interface issues between VHA medical devices and the EHR, and
- Unapproved communication modes used by facility staff that risk disclosure of sensitive personal information.

During this inspection, the OIG team identified two additional issues involving a possible breach of patients' sensitive personal information and the use of logbooks.

VA and VHA employ policies that safeguard the privacy of patient information and the release of information. VHA and facility policies must comply with all applicable privacy and confidentiality laws. Although several of these policies protect the release of information by individuals, additional policies are specifically in place to protect sensitive personal information from being released using information devices and communication systems, such as email systems and text messages. Staff working for VHA facilities must comply with privacy and confidentiality rules.[2]

The facility's high-resolution esophageal manometry (HRM) medical device lacked the ability to interface with VHA's EHR system beginning in 2013 when the VA upgraded from the Windows XP operating system to Windows 7.[3] With this upgrade, the VA IT network (network) could no

[1] Interface is defined as the place at which independent and often unrelated systems meet and act on or communicate with each other.

[2] VHA Directive 1605.01, *Privacy and Release of Information,* August 31, 2016. VHA defines sensitive personal information as, any information about the individual maintained by VA that includes, "(1) education, financial transactions, medical history, and criminal or employment history; and (2) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records."

[3] HRM of the esophagus is a technique that provides a precise assessment of esophageal motility, such as swallowing and sphincter controls. It measures the entire length of the esophagus and is thought to take less time and be more accurate than other diagnostic tests.

longer support the software interface between the facility HRM and the EHR. The gastroenterology (GI) provider stated that, along with the facility Biomed and IT, a decision was made to continue to use the facility's HRM without the ability to interface with the patients' EHR. Based on this decision, the GI provider developed and implemented two workarounds that were not in accordance with VA security and privacy policies concerning sensitive personal information. These workarounds included the use of the GI provider's personal computer and emails, a non-VA (unencrypted) flash drive, and the Cloud.[4]

Besides the HRM, 8 of 11 other medical devices also lacked the ability to interface with the EHR. However, the providers and staff using these medical devices in the GI laboratory, neurology, and pulmonary/sleep laboratory developed workarounds that ensured the secure transfer of data, results, and images from the medical devices to the EHRs.[5]

Biomed and IT initially assisted the GI provider with resolving the facility HRM's inability to interface with the EHR. However, according to the GI provider, Biomed and IT did not address additional software interface issues, therefore, the GI provider developed workarounds to transfer patient information from the facility HRM to the EHR. The OIG could not confirm the GI provider's statements regarding assistance requests as the GI provider did not have documentation of the requests and the identified Biomed staff member no longer worked for the facility. Although the OIG identified the HRM work order and lack of interface with the patients' EHR, the OIG noted a lack of discussion or at least documentation between the GI provider, Biomed, and IT on how the GI provider would transfer data from the facility HRM to the EHR.

The OIG established that the providers and staff in GI laboratory, neurology, and pulmonary/sleep laboratory developed their own workarounds to transfer information into the patient's EHR when their medical devices could not interface with the EHR. The OIG did not find that these providers or staff relied on Biomed or IT for assistance with developing their workarounds.

Although staff, including the GI provider, were aware of the importance to secure patients' sensitive personal information, one staff member sent unencrypted emails, and staff sent text messages and text pages. The OIG identified that 99 percent of emails sent from the GI provider's personal email account and 91.7 percent of text messages between the GI provider and staff contained patients' sensitive personal information.

The OIG concluded that the outpatient clinic and lab nursing staff and providers preferred mode of communication was the telephone, but if sending a text message, the nursing and clinic staff

[4] Cloud refers to the storing of computer data on multiple servers that can be accessed through the internet. The software used to store the information is not on the computer's hard drive.

[5] The 11 devices the OIG reviewed included the colonoscope, upper GI endoscope, pulmonary function, and sleep testing equipment.

stated the text messages stated, “call me,” “patient here,” and “come to clinic.” The inpatient nursing and unit staff preferred mode of communication was text pages utilizing SPOK.[6] Although the OIG found that inpatient nursing and unit staff sent patients’ sensitive personal information through the non-secured SPOK system, the OIG believes that it is plausible that the nursing and unit staff either overlooked the warning, or possibly assumed that because they could access the SPOK system through the facility’s intranet site, that it was a secure system.

The information system security officer (ISSO) and the privacy officer had a difference of opinion when asked what constituted sensitive personal information. For example, when asked if a text message containing a patient’s first initial of the last name and the last four of the social security number (for example A1234) was appropriate, one agreed that information was acceptable to use while the other viewed it as sensitive personal information and should not be sent over a text message. The ISSO advised staff to use the least amount of information necessary to conduct business and to encrypt messages that contained sensitive personal information and stated that staff should use their own judgment when making that determination.

After the OIG discovered the GI provider’s work around for the HRM, the ISSO entered and tracked a missing/stolen equipment report/ticket in the privacy and security event tracking (PSET) system. However, the OIG determined that the information submitted by the ISSO appeared limited and incomplete as it did not identify a possible breach of patient sensitive personal information. Based upon the information submitted by the ISSO, the VA Network and Security Operations Center (NSOC) provided no guidance to the facility.

Upon further review, the OIG identified 133 patients who had sensitive personal information mentioned in the GI provider’s personal emails and text messages. The OIG requested that the Facility Director consider what, if any actions need to be taken to address this incident. The Facility Director had the privacy officer enter a new PSET system ticket for mishandled information with additional data. However, the Facility Director provided the OIG with an email that the data breach response service did not consider this incident a breach as no evidence was provided that the sensitive personal information had been lost or disclosed to unauthorized persons. Because it was not considered a breach, the 133 identified patients were not notified of a possible disclosure and would not be offered credit monitoring.

OIG staff concluded that, although there was no evidence that unauthorized persons accessed patient sensitive personal information, the GI provider and facility staff increased the risk and possibility that sensitive personal information for the 133 patients could have been disclosed or accessed by unauthorized persons.

[6] SPOK is an online alphanumeric paging system used almost exclusively on the inpatient units.

In addition, although the VA handbook that addressed guidance to sensitive personal information incidents and events was revised March 29, 2019, the OIG identified that the handbook does not address the issues identified in this report.

During the inspection, the OIG found that facility staff used two physical logbooks that tracked testing equipment taken home by patients and contained patients' sensitive personal information. The use of physical logbooks violates VHA policy.

The OIG made six recommendations related to communication and education, disclosure of protected patient information, VHA policy review, and compliance with the use of logbooks.

Comments

The VA Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer, and the Veterans Integrated Service Network and Facility Directors concurred with the recommendations and provided acceptable action plans for recommendations 1–4 and 6. (See appendixes A, B, and C, pages 26–32 for the VA Principal Deputy Assistant Secretary and Directors' comments.) The OIG considers all recommendations open (see discussion below related to recommendation 5) and will follow up on the planned actions until they are completed.

OIG Response to the VA Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer Comments

The VA Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer concurred with recommendation 5; however, stated that current VA policy, addressed the most common privacy breaches or events on a case by case basis, and that it was impractical to incorporate every privacy and security event. The OIG agrees that current policy advises employees to not use personal devices without permission; however, the OIG identified a lack of VA guidance to the facility when addressing the security ramifications of transmitting sensitive personal information using personal devices. The OIG considers this recommendation open for VA to address the lack of VA guidance to avoid mismanagement of sensitive personal information using personal devices.

JOHN D. DAIGH, JR., M.D.
Assistant Inspector General
for Healthcare Inspections

Contents

Abbreviations

EHR	electronic health record
GI	gastroenterology
HRM	high-resolution manometry system
ISSO	information system security officer
IT	information technology
NSOC	Network and Security Operations Center
OIG	Office of Inspector General
PSET	privacy and security event tracking system
USB	universal serial bus
VAMC	VA Medical Center
VHA	Veterans Health Administration
VISN	Veterans Integrated Service Network

Introduction

The VA Office of Inspector General (OIG) conducted a healthcare inspection in response to issues involving episodes of non-adherence to Veterans Health Administration (VHA) and VA policies on patient information privacy and security identified during an unrelated OIG investigation at the Tibor Rubin VA Medical Center (facility), Long Beach, California.

Background

The facility, part of Veterans Integrated Service Network (VISN) 22, consists of five community based outpatient clinics located in Anaheim, Laguna Hills, Santa Ana, Santa Fe Springs, and Villages at Cabrillo in Long Beach. The facility also operates two Vet Centers located in Garden Grove and Mission Viejo. From October 1, 2016, through September 30, 2017, the facility served 55,315 patients and had a total of 401 operating beds, 291 inpatient beds, and 110 community living center beds. The facility provides acute inpatient care for medicine, mental health, surgery, and spinal cord injury and disorder, and outpatient services in primary care, specialty care including gastroenterology (GI), neurology, and pulmonary, and long-term care in the areas of blind rehabilitation center, community living center, and spinal cord injury and disorder.

VHA Processes to Safeguard Patient Information

With the ongoing advancement in technology, health care systems, including VHA, are continually challenged to ensure the protection of patient privacy and security of their health care information. VA and VHA issued policies to safeguard the privacy of patient information and the release of information. VHA and facility policies must comply with applicable privacy and confidentiality laws. Although several of these policies protect the release of information by individuals, additional policies are specifically in place to protect sensitive personal information from being released using information devices and communication systems, such as email and text messages.[7]

[7] VHA Directive 1605.01, *Privacy and Release of Information,* August 31, 2016; VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, July 28, 2016. This handbook was rescinded and replaced with VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, March 12, 2019. Unless otherwise noted, the two handbooks contain the same or similar language; VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,* March 10, 2015; VA Office of Information Security, Field Security Service, "FSS Guidance – Text Messaging," Bulletin FSS No. 83, January 30, 2013.

Protection and Privacy of Sensitive Personal Information

VHA defines sensitive personal information as, any information about the individual maintained by VA that includes: "(1) education, financial transactions, medical history, and criminal or employment history; and (2) information that can be used to distinguish or trace the individual's identity, including name, social security number [SSN], date and place of birth, mother's maiden name, or biometric records."[8] The term sensitive personal information is inclusive of personal identifiable information and protected health information.[9]

VA policy states that users of VA information systems or VA information are responsible for complying with VA National Rules of Behavior.[10] Those rules state that, VA employees "will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and authorized in advance," by the appropriate VA official and a waiver has been issued by the VA's Chief Information Officer.[11] In addition, VA employees "will not access, transmit, or store remotely any VA sensitive information that is not encrypted using VA-approved encryption."[12]

VHA, as the owner of VHA patient information, approves and provides access to sensitive personal information in the VA information technology (IT) systems and is required to employ reasonable technological safeguards to protect sensitive personal information that is stored electronically. Individuals that are approved and meet VA and VHA requirements (such as training and need for access) will be granted access to VHA data processed and stored on VA IT systems. However, this policy does not encompass VHA sensitive personal information contained in medical devices or paper records.[13]

Emails

According to VA policy, VA email communication system must be used for authorized government purposes and contain only non-sensitive information, unless the information is encrypted. The VA Office of Information and Technology oversees the encryption process.[14] The

[8] VHA Directive 1605.01.

[9] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[10] VA Handbook 6500.

[11] VA Handbook 6500.

[12] VA Handbook 6500, VA defines encryption as the process of changing plaintext into ciphertext for security or privacy.

[13] VHA Directive 1080, *Access to Personally Identifiable Information in Information Technology Systems*, January 6, 2017.

[14] VA Handbook 6500.

VA Rules of Behavior state that employees will use VA-approved encryption for any email that contains VA sensitive information, including sensitive personal information.[15]

Text Messages

According to the VA Office of Information Security, employees may use text messages in the same manner as using emails in the performance of their job duties; however, because of the absence of guaranteed encryption with text messages, employees should not utilize text messages to transfer VA sensitive information including sensitive personal information.[16]

Medical Devices

VA policy recognizes that sophisticated medical devices designed with the added capacity to store patient data and be connected to the VA IT network (network) provides many benefits such as the quick delivery of data and images from diagnostic procedures to clinical staff. The prompt delivery of data enables clinical staff to provide more effective and efficient care, but also increases the risk of exposing sensitive personal information to users who should not view that data. In addition, medical devices that are not connected to the network may store patient data which could be lost or stolen, or staff may develop workaround processes to transfer data from the medical devices to the electronic health record (EHR) without ensuring the data is encrypted. Medical devices shall be assessed for technology compliance with the network before being acquired, and the assessment shall address the risk of compliance issues and the most effective way to integrate the equipment into a facility's operations.[17]

Privacy Officers' and Information System Security Officers' Responsibilities

Privacy officers are responsible for taking protective measures to help ensure that sensitive personal information collected by VA is limited to that which is legally authorized and necessary, thereby minimizing the exposure of patient sensitive personal information. The privacy officer also assists in reporting misuse and mitigating damage when sensitive personal information is or potentially compromised or disclosed.[18]

The information system security officer (ISSO) ensures that operational security is maintained for information systems as required by VA and facility policy.[19] The ISSO's responsibilities

[15] VA Handbook 6500.

[16] VA Office of Information Bulletin FSS No. 83.

[17] VA Directive 6550, *Pre-Procurement Assessment for Medical Device/Systems*, February 20, 2015.

[18] VA Handbook 6500.

[19] VA Handbook 6500 defines information systems as, "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual." Facility Policy IM-01, *Information Security Program*, June 13, 2016.

include notifying the VA national security office of any confirmed or suspected incident within one hour of discovery, assisting in the incident investigation if needed, providing official guidance on information security matters to facility management and staff, and ensuring compliance with federal security requirements and VA security policies.[20]

Sensitive Personal Information Incident, Breach, and Disclosure

To ensure compliance with federal privacy laws and to prevent unauthorized disclosures of sensitive personal information, VA established procedures to determine if an incident or a breach occurred within VA information systems.[21] VA defines an incident as, "any event that has resulted in, or has the potential to result in, unauthorized access to or disclosure of VA [sensitive personal information] in a manner not permitted under the applicable confidentiality provisions."[22] VA defines a breach as, "the acquisition, access, use, or disclosure of VA [sensitive personal information], including PII [personally identifiable information] and PHI [protected health information], in a manner not permitted by law or VA policy which compromises the security or privacy of the [sensitive personal information.]"[23] A data breach, per 38 U.S.C. § 5727(4), is "the loss, theft, or unauthorized access, other than those incidental to the scope of employment, to data containing [sensitive personal information], in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data."[24]

A breach is determined using VA policy that focuses on VA printed and electronic sensitive personal information sent and read or potentially read by non-VA persons, or VA staff who had no need to view the information, and/or a loss of VA equipment or sensitive personal

[20] VA Handbook 6500. In addition, the ISSO reviews contracts to ensure security is defined, manages facility information security programs, and serves as the principal security advisor to information owners regarding security consideration in information applications and systems, such as the electronic health record, and procurement, development, implementation, operation, maintenance, and disposal activities; coordinating, advising, and participating in the development and maintenance of security system plans.

[21] Based upon VA policy, an incident is any event that has resulted in or has the potential to result in unauthorized access to or disclosure of VA sensitive personal information in a manner not permitted under the applicable confidentiality provisions.

[22] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.The 2019 definition of an incident is similar to the 2016 definition with the additional explanation added: "An incident is any occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

[23] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019. The 2019 definition of a breach is similar to the 2016 definition with the additional explanation added: "loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where i. a person other than an authorized user accesses or potentially accesses personally identifiable information or ii. an authorized user accesses or potentially accesses personably identifiable information for another than authorized purpose."

[24] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019. Compromise, in this context, means the loss of VHA sensitive information.

information that cannot be recovered. The VA process to determine a breach involves three parts:

1. Identifying whether an incident that exposed or had the potential to expose sensitive personal information has occurred. [25]
2. Analysis of the exposure risk. This is determined using VA policy breach criteria for specific circumstances (called Standard Risk Assessment Matrices) that identifies if patient sensitive personal information was exposed to an unauthorized person (non-VA or VA staff) that have no need to view the information. For example, if the possible breach is categorized as mishandling of sensitive personal information, the sensitive personal information must be lost and the exposure unknown, or the sensitive personal information contents exposed to anyone who was not a veteran, veteran family member, or VA staff. The initial example would be considered a breach, the last example would trigger a complete/full risk assessment (see below).[26]
3. Assess additional risk of exposure if the standard risk assessment matrix criteria does not clearly identify a breach. VA policy states that "an acquisition, access, use, or disclosure of SPI [sensitive personal information] is presumed to be a breach, unless VA demonstrates there is a low probability the SPI [sensitive personal information] has been compromised based on a risk assessment of factors." This assessment includes the length of time the information was possibly exposed, whether the sensitive personal information was viewed or used, and the ease of logical access to sensitive personal information considering the degree of protection.[27]

Once VA staff determines a breach occurred, additional procedures are used to determine whether VA should notify or offer credit protection services to individuals whose sensitive personal information has been or may have been exposed. The primary goal of these policies and procedures is to provide prompt and accurate notification and remediation, if necessary.[28]

In accordance with the VA Office of Information and Technology procedures, when a complaint is made, the privacy officer or ISSO will begin to investigate and within one hour of the notification, enter a ticket/report of the possible incident into the privacy and security event

[25] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[26] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[27] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019. A risk assessment includes "(a) The nature and extent of the SPI [sensitive personal information] involved…; (b) The unauthorized person who acquired, accessed or used the SPI [sensitive personal information], or to whom the disclosure was made; (c) Whether the SPI [sensitive personal information] was acquired or viewed; and (d) The extent to which the risk to the [SPI] [sensitive personal information] has been mitigated."

[28] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

tracking (PSET) system.[29] The privacy officer or ISSO will continue to investigate the complaint and report back to the VA Data Breach Response Service every 72 hours until the complaint or incident is closed.[30] VA Handbook 6500.2 states, "If a breach has occurred, the DBCT [Data Breach Response Service] will follow the breach management process and determine the level of risk and whether notifications and credit protection services are warranted."[31]

If sensitive personal information is compromised, corrective and mitigating actions include employee training, revising policies and procedures to prevent a reoccurrence, and providing notifications or credit protection services to individuals whose sensitive personal information was involved in the incident. A full review should be done before closing the incident by evaluating how staff and management responded and confirming closure by addressing the incident in writing.[32]

VHA Equipment Procurement and Access Processes for Medical Devices

Procurement

VA Directive 6550 establishes that a pre-procurement assessment be completed by a facility's technical support services, consisting of biomedical engineering (Biomed), IT, and the ISSO, for any medical device that will be connected to the network or for medical devices that will store sensitive personal information.[33] "Evaluating the configuration and security profile of medical devices during the [pre-procurement] process will identify potential risks and ultimately provide for more effective and safe integration of medical devices into hospital operations."[34] Prior to the delivery of the medical device, Biomed coordinates the implementation planning process with the assistance of IT, ISSO, engineering, the requesting clinical service, clinical informatics (as required), and the vendor.

Network Access

To ensure privacy and security of the network, the VA must determine if a medical device can interface with the network and determine if that ability to interface poses a risk to either the

[29] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[30] The Data Breach Response Service is a national VA program that supports facilities and regional offices by providing breach incident response activities and guidance based upon the incident information in the PSET system. The Service performs analysis to determine the likelihood of a breach upon request of the facility or regional office.

[31] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[32] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[33] VA Directive 6550.

[34] VA Directive 6550.

network or the medical device.[35] Based on these determinations, VA may restrict and isolate medical devices from accessing the network. According to the facility's Chief of IT, network access consists of three options.

1. Direct Interface: Data, results, and images obtained from the medical device directly transmit into a patient's EHR.
2. Indirect Interface: Data, results, and images obtained from the medical device are initially saved as a document on another server and then uploaded into a patient's EHR.
3. No Interface: Some medical devices are unable to directly or indirectly interface with the EHR. In these cases, the information must be manually entered into a patient's EHR.

Request for Review

On May 16, 2017, the OIG received allegations regarding time-card fraud, kickbacks, conflicts of interest, and misuse of government funds by certain medical staff at the facility. Between July 10, 2017, and November 8, 2017, the OIG Office of Investigations investigated, but did not substantiate the allegations. However, the Office of Investigations identified and investigated an additional issue involving the potential violation of the VA information security policy. Specifically, the Office of Investigations concluded that a GI provider and other staff used methods to transfer, store and send patient information that did not protect patient sensitive personal information. On May 22, 2018, the OIG Office of Healthcare Inspections was tasked to review episodes of non-adherence to the VHA privacy and security policies. The specific areas of concerns were

- Lack of software interface between VHA medical devices and the EHR, and inappropriate staff workarounds.
- Lack of Biomed and IT assistance in resolving software interface issues between VHA medical devices and the EHR.
- Unapproved communication modes used by facility staff that risked disclosure of sensitive personal information.

During this inspection, the OIG team identified two additional issues for review. These two issues are the potential breach of 133 patients' sensitive personal information and the use of logbooks.

[35] Merriam-Webster defines interface as the place at which independent and often unrelated systems meet and act on or communicate with each other.

Scope and Methodology

The OIG initiated the inspection on May 22, 2018, and conducted a site visit the week of August 6, 2018.

The OIG reviewed relevant VHA and facility policies and practices related to information security, privacy, equipment procurement, and telecommunication. Other records reviewed included equipment subcommittee meeting minutes, relevant work orders, preventative maintenance reports, and procurement documents for medical devices, such as the facility high-resolution esophageal manometry (HRM) device used in GI. [36]

The OIG reviewed and compared the interface capabilities and staff workarounds for the facility HRM and 11 medical devices used in the GI laboratory, neurology, and the pulmonary/sleep laboratory.

The OIG interviewed more than 40 individuals including facility leaders, the ISSO, privacy officer, patient advocate, IT area manager, Chief of Material Management Logistics Procurement, Chief of Quality, Safety, and Value, Chief of Biomed, and providers and staff from the GI laboratory, neurology, and pulmonary/sleep laboratory. In addition, the OIG spoke with National VHA staff including the National Director for GI, privacy officer, health product support manager, Deputy Executive Director of Enterprise Security Operations, and Specialized Device Security Division Deputy Director.

In the absence of current VA or VHA policy, the OIG considered previous guidance to be in effect until superseded by an updated or recertified directive, handbook, or other policy document on the same or similar issue(s).

The OIG conducted the inspection in accordance with *Quality Standards for Inspection and Evaluation* published by the Council of the Inspectors General on Integrity and Efficiency.

[36] HRM of the esophagus is a technique that provides a precise assessment of esophageal motility, such as swallowing and sphincter muscle controls. The device measures the entire length of the esophagus and is thought to take less time and be more accurate than other diagnostic tests.

Sequence of Events Related to a Potential Breach in Patients' Sensitive Personal Information[37]

In July 2017, the OIG Office of Investigations identified and investigated an issue involving the potential violation of the VHA information security policies. Specifically, the GI provider and other staff used unauthorized methods to communicate, transfer, and store patients' sensitive personal information.

When a patient experiences reflux, constipation, or incontinence, a GI provider uses a medical device to measure swallowing and sphincter functioning. The medical device or HRM creates a Microsoft Word (Word) document that contains the study results and pictures. Within this Word document, a provider can type in their interpretation of the results. The GI provider noted the importance of pictures included in the Word document. The facility HRM used the Windows XP operating system and was able to interface with the EHR. The ability to interface allowed the GI provider to save study results as a document, and then upload it to the EHR.

In 2013 VA upgraded from the Windows XP operating system to Windows 7.[38] With this upgrade, the network could no longer support the interface between the HRM and the EHR. However, the HRM remained operational including producing a Word document that contained study results and pictures.

In 2013, the GI provider notified the direct supervisor, IT, and Biomed about the HRM's inability to interface with the EHR. Options discussed to address the problem included referring patients to the community through the Veterans Choice Program, purchasing a new HRM, or continuing to use the present facility HRM, but without the ability to interface with the EHR.[39] The GI provider, along with Biomed and IT, made a decision to continue to use the HRM, but without the ability to interface with the patients' EHR. The GI provider developed and implemented two workarounds to enter the HRM information into the EHR. The GI provider continued to use the facility HRM until it became non-operational around June 2018.

The GI provider explained the initial and secondary workarounds in using the facility's HRM. The GI provider used the initial workaround from 2013 through 2015.

[37] Unless otherwise indicated, information in the sequence of events was provided to the OIG during interviews with staff.

[38] According to Microsoft, support of Windows XP operating system ended April 8, 2014.

[39] The Veterans Choice Program is a VA program that allows patients to receive care in the community if the VA is unable to provide care in a timely manner or if the patient lives further than 40 miles from the nearest VA medical facility or it is too difficult for the veteran to get to the VA medical facility.

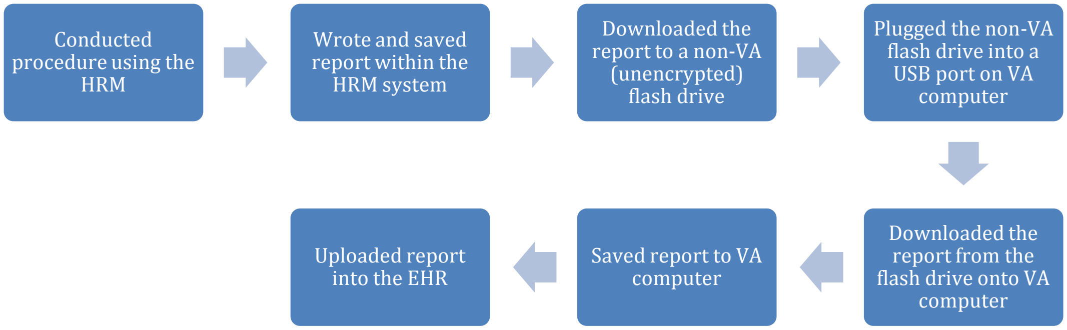
Conducted procedure using the HRM
Wrote and saved report within the HRM system
Downloaded the report to a non-VA (unencrypted) flash drive
Plugged the non-VA flash drive into a USB port on VA computer
Downloaded the report from the flash drive onto VA computer
Saved report to VA computer
Uploaded report into the EHR

Figure 1. GI Provider's Initial Workaround[40]
Source: VA OIG interview and analysis

Around 2015, VA disabled universal serial bus (USB) ports to devices not approved by VA. The GI provider could no longer use the non-VA (unencrypted) flash drive to transfer reports from the facility HRM to the VA computer. No additional information was available concerning IT interventions or interactions between the GI provider and IT. The GI provider then developed a secondary workaround to compensate for this change. The GI provider, acting alone and without guidance from the facility's privacy officer or ISSO, used a non-VA (unencrypted) flash drive, personal computer, and personal email account to transfer reports from the facility HRM to the VA computer.[41] The GI provider used the secondary workaround from 2015 through 2017. The GI provider deleted the VA emails and Word documents but did not check or delete the emails sent from personal email to the VA email account; and the emails remained in the sent box for the length of time this work around was used.

[40] A flash drive is a small portable storage device that connects to computers and other devices via a built-in universal serial bus (USB) port; A USB port is a standard cable connection on personal computers and other electronic devices. A USB port allows a flash drive to connect to a computer or other electronic devices to transfer data between the flash drive and the computer or other electronic device.

[41] This was a free Gmail account that was not approved by VA and that the GI provider set up for personal use for many purposes. The GI provider sent sensitive personal information in attachments that were not always password protected, and these emails with attachments were not deleted from the Gmail sent box so remained on-line, stored in the Gmail sent box throughout the time the provider used the Gmail account for these purposes.

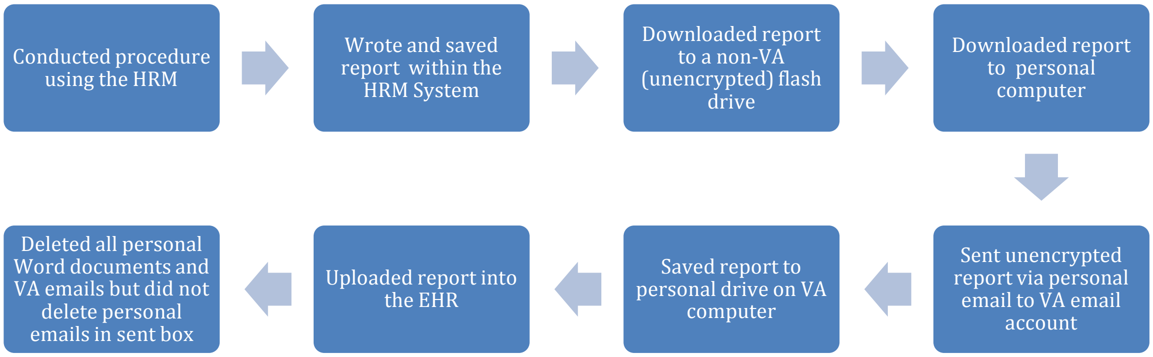
Conducted procedure using the HRM
Wrote and saved report within the HRM System
Downloaded report to a non-VA (unencrypted) flash drive
Downloaded report to personal computer
Sent unencrypted report via personal email to VA email account
Saved report to personal drive on VA computer
Uploaded report into the EHR
Deleted all personal Word documents and VA emails but did not delete personal emails in sent box

Figure 2. GI Provider's Secondary Workaround[42]
Source: VA OIG interview and analysis

In 2016, a second provider began using the HRM; however, this provider relied upon the GI provider to send patients' reports via VA-encrypted email. The second provider did not utilize the workarounds developed by the GI provider.

In August 2017, the Office of Investigations inspected the GI provider's laptops, personal email account, and Cloud storage and concluded that the GI provider did not follow VA information security policy regarding patient sensitive personal information by using these storage items.[43] The GI provider, in the presence of the ISSO, deleted personal emails and Cloud storage that contained sensitive patient information. For diagnostic purposes to continue to provide access to the HRM, the GI provider was issued a VA-encrypted flash drive to transfer reports from the facility HRM to the VA computer.

Around May 2018, the GI provider reported to the facility IT and Biomed departments that the facility HRM was no longer working and requested a new HRM. The scheduled patients were given the option to wait until a new HRM became available or be referred to another VA for the procedure. As of September 7, 2018, Biomed informed the OIG that the facility staff procured a new HRM and were in the process of making the equipment fully operational. While waiting for the HRM to be able to interface with the EHR, the GI provider informed the OIG that Biomed approved the use of the new HRM and to continue to use the VA-encrypted flash drive to transfer reports from the facility's new HRM to the VA computer.

[42] Over time, the non-networked medical device became more unstable, so the GI provider downloaded the report to the non-VA (unencrypted) flash drive and uploaded it to the personal computer where the GI provider would complete the report with interpretation.

[43] Cloud refers to the storing of computer data on multiple servers that can be accessed through the internet; the software used to store the information is not on the computer's hard drive.

Inspection Results

1. Lack of Software Interface Between VHA Medical Devices and the EHR and Staff Workarounds

Facility HRM

The OIG determined that the facility HRM lacked the ability to interface with the EHR beginning in 2013. In addition, the GI provider did not follow VA security requirements, under the VA Rules of Behavior, to secure and protect VA information, when developing and implementing the workarounds used when the facility HRM could no longer interface with the EHR. However, when the security risk was identified by OIG, the ISSO did take mitigating measures to decrease the risk of exposure to patient sensitive information.

The VA and facility established policies and procedures to ensure the protection and privacy of patients' sensitive personal information.[44] To accomplish compliance with VA policies and ensure VA employees are knowledgeable users, VA requires employees to review and sign the VA's Rules of Behavior when they begin working for the VA.[45] The Rules of Behavior define the responsibilities and expected behaviors of employees who use the VA system or who have access to VA information. The GI provider admitted probably doing the annual privacy training as required of VHA employees, which includes the Rules of Behavior.

Based on interviews with the GI provider, the OIG determined that due to the VA 2013 upgrade to Windows 7, the facility could no longer establish an interface between the HRM, which used Windows XP, and the EHR. In response, the GI provider, Biomed, and IT discussed other available options to provide patient care and decided to continue to use the facility HRM without the interface capability.

Based on this decision, the OIG found that the GI provider developed two workarounds, as described above, that were not in accordance with the VA's Rules of Behavior or VA policy. Specifically, the GI provider, without authorization, uploaded and downloaded information on VA systems, allowed VA sensitive personal information to reside on non-VA systems (including unencrypted email systems with Cloud storage and devices such as unencrypted flash drives), and sent unencrypted emails from a personal email system containing VA sensitive information to VA accounts.

When the OIG initially identified the security risk, the facility security staff mitigated the issues by deleting sensitive personal information from the GI provider's email and storage accounts,

[44] VA Handbook 6500; Facility Policy IM-02, *Access Policy*, January 25, 2018.

[45] VA Handbook 6500; Facility Policy IM-02.

and then provided an encrypted protected VA flash drive to the GI provider. In addition, the facility security staff filed and updated a ticket in the PSET system.

Facility GI Laboratory, Neurology, Pulmonary/Sleep Laboratory Departments

The OIG determined that additional medical devices lacked the ability to interface with the EHR. However, the providers and staff using these medical devices developed workarounds that ensured the secure transfer of data, results, and images from the medical devices to the EHRs.

To determine the interfacing capability of other medical devices and workarounds developed by staff, the OIG reviewed 11 medical devices used in the GI laboratory, neurology, and the pulmonary/sleep laboratory.[46]

Three of the 11 medical devices either directly or indirectly interfaced with the EHR. For the remaining eight medical devices, the OIG was informed through various staff interviews that although the devices did not interface with the EHR, the staff developed workarounds that ensured the secure transfer of information from the medical device to the EHR. For seven of the medical devices, the workarounds included manual entry of the data from the medical device to the EHR by a provider or staff member. For the other medical device, a report was printed from the device, then scanned with VA equipment to a VA computer and sent to the technicians' VA email account. The technician saved the report on a protected facility intranet shared drive and imported the report into the EHR.[47]

2. Lack of Biomed and IT Assistance in Resolving Software Interface Issues Between VHA Medical Devices and the EHR

Facility HRM

The OIG determined that Biomed and IT initially assisted the GI provider with resolving the facility HRM's inability to interface with the EHR. Although the GI provider stated that Biomed and IT did not address ongoing issues, the OIG did not find any further work orders, requests, or documentation related to software interface issues and could not determine whether facility Biomed and IT staff provided additional support.

VHA requires EHR documentation to record pertinent facts and findings, including examinations, tests, and treatments. In addition, VHA requires all patient care records be stored in the patient's EHR through direct documentation, scanning, or other emerging technologies

[46] The 11 devices the OIG reviewed included colonoscope, upper GI endoscope, pulmonary function, and sleep testing equipment.

[47] In addition, the OIG team found that five of the eight non-interfacing medical devices stored patient information, but they were password protected and located in locked rooms.

(such as diagnostic software that directly or indirectly interfaces with the EHR). Providers performing diagnostic procedures must document detailed reports, including findings and conclusions, in the patient's EHR.[48]

The OIG team reviewed the IT work and new equipment orders from 2012 through 2017 and found the January 16, 2013, HRM Windows upgrade work order. This work order included discussions of options and the decision to continue to use the facility HRM without the ability to interface because an alternative could not be found. Per the work order, the facility's IT Committee approved the decision to continue to use the facility HRM; however, the work orders had no additional documentation regarding how the provider could use the HRM without the interface. Because of this decision, the GI provider developed and implemented the initial workaround, which include the transfer of information from the HRM to the EHR via a non-VA (unencrypted) flash drive. The OIG team found two additional work orders for new HRM catheters in April 16, 2013, and June 11, 2014.

When further problems with the facility HRM developed in 2015, the GI provider stated that Biomed did not respond to the concerns. The OIG could not confirm the GI provider's statement because the GI provider could not produce documentation of the request for assistance, and the Biomed staff member, to whom the GI provider referenced, no longer worked for the facility. In addition, the GI provider stated that the direct supervisor, who left in April 2017, was aware of these issues, but was not helpful or interested. In 2015, the GI provider developed and implemented the secondary workaround, which included the use of a personal computer and email, non-VA (unencrypted) flash drive, and Cloud storage.

Based on the review of IT work orders and interview with the GI provider, the OIG noted a lack of documented discussion between the GI provider, Biomed, and IT of how the GI provider would transfer the data from the facility HRM to the EHR.

Facility GI Laboratory, Neurology, Pulmonary/Sleep Laboratory Departments

The OIG found that the providers and staff within the GI laboratory, neurology, and pulmonary/sleep laboratory developed their own workarounds to input information into the patients' EHR when their medical devices could not directly or indirectly interface with the EHR. The OIG did not find that these providers or staff relied on Biomed or IT for assistance with developing their workarounds.

[48] VHA Handbook 1907.01, *Health Information Management and Health Records*, March 19, 2015.

3. Unapproved Staff Communication Modes that Risk Disclosure of Sensitive Personal Information

The OIG determined that although staff were aware of the importance to secure patients' sensitive personal information, one facility staff member sent unencrypted emails, and staff members sent unencrypted text messages, and text pages.

Communication Modes

Emails

The OIG determined that the GI provider did not follow the VA Rules of Behavior when emailing patient HRM information from personal email or sending unencrypted emails.

In August 2017, the OIG subpoenaed copies of the GI provider's relevant personal email messages. Following the site visit in August 2018, the OIG reviewed the 100 unique personal email messages provided by the GI provider and determined that 99 (99 percent) contained sensitive personal information consisting of a combination of last name or last name initial, first name or first name initial, date of birth, and full or partial SSNs. The remaining email message contained a patient's last name.

According to interviews, the GI provider used a personal email system that was set up for other purposes besides VA business.[49] The GI provider sent attachments with patient sensitive personal information, including test results, in these personal emails that were not protected by encryption. The GI provider never checked the sent box for these emails and never deleted the emails in the sent box. Therefore, these unencrypted emails and attachments with sensitive personal information remained on the personal email site through the time period the GI provider used the second work around. The length of time the unencrypted emails remained on the email site increased the risk and possibility that unauthorized persons accessed sensitive personal information.

Text Messages

The OIG determined that the GI provider and some facility staff sent unencrypted text messages to transmit test result information that included patients' sensitive personal information.

On January 30, 2013, the VA Office of Information Security, Field Security Service, issued a bulletin stating that VA employees may use text messages to perform their job duties in the same manner they would use emails; however, because of the absence of encryption in text messaging, an employee should not utilize text messages to transfer sensitive personal information.[50] The

[49] This was a free Gmail account that was not approved by VA and that the GI provider set up for personal use for many purposes.

[50] VA Office of Information Security Bulletin No. 83.

VHA privacy officer confirmed that text messages are not encrypted, even when sent between two VA cell phones.

During an interview in September 2017, a facility nursing staff member stated that staff sent text messages from their personal cell phones to the GI provider's personal cell phone concerning tests results. These results included sensitive personal information to help move the patients through the testing process. When interviewed, the staff member reported no one, including the GI provider, told staff to text message test result to the GI provider. The nursing staff member also reported sending test results through text messages at their previous non-VA position.

In August 2017, the OIG subpoenaed copies of the GI provider's relevant text messages. Following the site visit in August 2018, the OIG reviewed 36 unique text messages and determined that 33 (91.7 percent) text messages contained sensitive personal information consisting of a combination of last name, first name or first initial, date of birth, medical information, and full or partial SSNs. The remaining three text messages contained either the patient's last name and unit/room number or just the patient's last name.

During the August 2018 site visit, the GI provider confirmed that staff had text messaged test results with sensitive personal information. The GI provider related speaking with staff and this was no longer occurring. However, the unapproved use of the text messaging system on the GI provider's and other staff's personal cell phones increased the risk that patient sensitive personal information could be disclosed to unauthorized or non-VA staff.

To confirm if the issue of text messaging providers was unique to the GI laboratory and the GI provider, OIG interviewed providers and staff located in the GI laboratory, specialty care clinics, neurology, pulmonary/sleep laboratory, and the inpatient units.[51]

The OIG team interviewed 24 providers and staff to determine if text messaging sensitive personal information was a common practice throughout the facility. The OIG team asked the providers and staff about the modes of communication they use, information disclosed specifically over text messaging and the SPOK (online alphanumeric paging system) system, and if they have or would ever text message pictures of lab results or wounds (as examples) with patient information to another VA provider.

The OIG found that the providers and staff used a variety of communication modes including telephone calls, instant messaging, numeric paging, text messages, and SPOK. Outpatient clinic, laboratory staff, and the providers preferred to communicate via the telephone, followed by text messages, and paging. Nursing and clinic staff stated the information they text messaged to providers included "call me," "patient here," and "come to clinic." Inpatient nursing and unit staff preferred to communicate with providers through the SPOK system followed by telephone calls, paging, and text messages. The providers and staff uniformly stated they have never nor

[51] The inpatient units included medicine/surgery on the fourth and eighth floors, the intensive care unit, the direct observation unit, and the progressive care unit.

would they ever text message photographs with patient information including lab results or wounds.

Text Pages

The OIG determined that inpatient staff were sending patient sensitive personal information when using the SPOK system to send text pages.

SPOK is an online alphanumeric paging system used almost exclusively on the inpatient units. According to the facility's IT area manager, SPOK is a national contract that provides alphanumeric pagers to several VA medical centers including the facility. The SPOK system is not a secure paging system and the facility's intranet site that leads to the SPOK system states "NOTE: Do not include PII [personally identifiable information]."

During the nursing and unit staff interviews, the OIG found that the inpatient nursing and unit staff used a combination of sensitive personal information including patient last name, patient first name, partial SSNs, unit location, room or bed number, and a brief description of the problem. Although the OIG found that inpatient nursing and unit staff transferred sensitive personal information through the SPOK system, the OIG believes that it is plausible that the nursing and unit staff either overlooked the warning, or possibly assumed that because they could access the SPOK system through the facility's intranet site, it was a secure system.

Determination of Sensitive Personal Information

Although VA defines what is sensitive personal information, the OIG asked the ISSO and privacy officer for clarification and examples of appropriate information that could be sent over text messages and SPOK.[52] The ISSO and the privacy officer provided different descriptions of what they considered to be sensitive personal information. When asked if a text message containing a patient's first initial of the last name and the last four of the social security number (for example A1234) was appropriate, one agreed that that information was acceptable to use while the other viewed it as sensitive personal information and should not be sent over a text message.

According to VHA's privacy officer, the privacy officer determines what is sensitive personal information, while the ISSO determines if there is a security violation involving sensitive personal information. The ISSO stated advising staff during new employee orientation to use the least amount of information to conduct business and to encrypt messages that contain sensitive personal information. When asked if the ISSO could provide examples, the ISSO responded advising that staff should use their own judgment. Because of variability of judgment, more specific guidelines or examples could assist staff to ensure they do not inadvertently send sensitive personal information over unsecure systems.

[52] VA Handbook 6500.

4. Possible Breach of Information

The OIG determined that 133 patients may have had their sensitive personal information disclosed to unauthorized persons when the GI provider stored unencrypted emails on non-VA systems, and the GI provider and facility staff sent text messages using personal cell phones.

VA identifies the primary goal of managing breaches of sensitive personal information, "…is to provide prompt and accurate notification and remediation, if necessary, to those individuals whose SPI [sensitive personal information] may have been inappropriately accessed, used, or disclosed in a manner not permitted by applicable confidentiality provisions."[53] In the event patient sensitive personal information has been or may have been disclosed, VA provides guidelines on how to address the breach or potential breach of information.[54] VA states that if the privacy officer, or ISSO, receive notice of an incident involving the possible compromise or loss of any VA sensitive information, they are to

- Enter all complaints (tickets) received within one hour of the discovery into the PSET system.[55]
- "Investigate the privacy or security incident and provide feedback to the Data Breach Response Service" and conduct a fact-finding investigation to determine validity of the complaint.[56]
- Execute any directions provided by the Data Breach Response Service, VA Network and Security Operations Center (NSOC), law enforcement, and the OIG.[57]
- Monitor and provide updates on any open or pending PSET system ticket.[58]
- Track the progress of response activity, if it is determined that a breach occurred.[59]
- Notify and keep facility leaders and relevant staff apprised of the incident.[60]

[53] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[54] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[55] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[56] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[57] The VA Data Breach Response Service uses VA breach criteria to determine if a breach occurred, if the person should be notified of the breach, and if credit protection service should be offered; VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[58] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[59] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[60] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

- The privacy officer prepares the incident notification/credit monitoring letters and obtains a promotion code for credit monitoring, when applicable.[61]

The privacy officer and ISSO are to coordinate efforts to determine if the detected or reported incident involves actual security and privacy violations. The data breach response service determines if a breach occurred based on available facts. If a breach occurred, the data breach core team will follow the breach management process, determine the level of risk, and determine if credit protection services are warranted.[62]

On August 1, 2017, the OIG notified the ISSO of an incident possibly involving sensitive personal information. The ISSO explained that their responsibilities include verifying if a violation occurred, notifying NSOC of the incident, submitting a PSET system ticket for review, notifying the privacy officer if sensitive personal information is present, and notifying facility leaders of the incident.

On August 2, 2017, the ISSO entered a PSET system ticket and updated the ticket until closure on October 31, 2017. On September 1, 2017, the ISSO notified the OIG that the facility has taken the following mitigation actions:

- The ISSO monitored the deleting of files containing VA data from the GI provider's personal email and Cloud storage.
- The GI provider was issued a VA-encrypted flash drive to transfer files from the facility HRM to a VA computer.
- The facility HRM exam room was rekeyed.
- The GI provider and Biomed reviewed options to determine a compliant replacement for the device currently in use.

During an OIG follow-up interview in August 2018, the ISSO explained the actions taken since being notified including interviewing the GI provider, meeting with Biomed, discussing the continued use of the facility HRM while ensuring the secure transfer of patients' sensitive personal information from the facility HRM to the EHR, and locating the facility HRM in a secure environment. The ISSO could not recall the number of patients involved in the possible breach. The ISSO also stated the NSOC generally will provide guidance on how to proceed with a sensitive personal information disclosure incident but did not do so in this circumstance.

The OIG reviewed the PSET system ticket, and found the ticket was categorized as "Missing/Stolen Equipment." The following are relevant entries noted on the PSET system ticket:

[61] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[62] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

- August 2, 2017 – The ISSO initially entered that the GI provider "…was using personal unencrypted laptop to transfer patient information from a medical device to VA systems, inappropriate transmission took place for at least one year."
- August 2 – The ISSO entered that they will interview the GI provider "…to assess the magnitude/type of information that may have affected patients." No information was documented that the interview occurred or the results of an interview concerning patients' sensitive personal information.
- August 3 – A VA Central Office employee entered, "Ticket involves possible security violation/privacy violation."
- August 4, August 11, and September 11 – The ISSO entered that the GI provider turned in the personal laptops and personal flash drive to the VA police.
- August 30 and September 1 – The ISSO entered that they are applying mitigation steps and positive remediation steps.
- September 13 – The ISSO entered the witnessing of the "scrubbing" of the GI provider's Cloud storage that contained VA patients' data.
- September 26 – The ISSO entered that "Mitigating actions have been applied to minimize impact to the organization."
- October 31 – The ISSO noted that, "All remedial steps… have been applied satisfactorily" and requested closing the PSET system ticket if NSOC had no further requirements.

The PSET system ticket did not include information concerning unencrypted personal emails or text messages possibly containing sensitive personal information. Although a VA Central Office employee identified that the incident possibly involved a security/privacy violation, no further discussion with the GI provider or actions were documented on the ticket. NSOC provided no additional documentation on the ticket about the possible breach of sensitive personal information or guidance.

The ISSO stated that it was the responsibility of the privacy officer to determine if patient information is at risk. The ISSO stated that there was the potential for patient information to be compromised, but that there is no evidence this occurred because no patient filed a complaint stating that their information was compromised.

When interviewed, the privacy officer reported being informed of the incident from the ISSO, but not monitoring or updating the PSET system ticket because the ISSO was the one who entered and updated the ticket. In addition, the privacy officer stated not being aware that sensitive personal information was involved in the incident and that, had the privacy officer known, could have entered an additional ticket concerning the sensitive personal information.

The Facility Director stated being informed of the incident by the ISSO and that the ISSO determined that only three patients may have had their information compromised. The Facility Director was unsure if the patients had been notified or how the ISSO made this determination.

The OIG requested that the Facility Director and the privacy officer review the incident to determine if patient sensitive personal information was compromised. The Facility Director reported on August 22, 2018, that obtaining information and identifying patients who may have been impacted was not possible because patient information was deleted from the GI provider's personal emails, and Cloud storage.

The OIG subpoenaed the GI provider's relevant personal emails and text messages and compiled a list of those patients mentioned. The lists consisted of 133 patients including three patients that were mentioned in both personal email and text messages. The OIG spoke with the Facility Director on September 13, 2018, regarding the compiled patient list and concerns about the possible compromise of sensitive patient information. The OIG sent the patient list to the Facility Director the following day and requested that the Facility Director consider what, if any, actions need to be taken and to provide a response on the decision.

On October 22, 2018, the Facility Director provided an email chain that showed on September 14, the privacy officer entered a new PSET system ticket for mishandled data. According to information provided by the facility, the PSET system ticket did not specifically address the GI provider's personal unencrypted email storage or text messaging, although it did address the unencrypted personal laptops and Cloud storage. The privacy officer contacted and requested guidance from the National Data Breach Response Service on September 19 for the 133 identified patients.

On October 5, the data breach response service stated that they did not consider this reported incident to be a data breach because the data was not disclosed to anyone besides VA staff. On October 18, the Facility Director requested whether credit monitoring could be offered to those identified patients. On October 22, the data breach response service stated they would only authorize credit monitoring if they determined a breach occurred. Since the GI provider was a trusted VA employee and did not lose the laptop or share patient information with anyone else, the information provided on the ticket was not considered a breach.

OIG staff reviewed the data for the 133 patients based on a complete/full risk assessment because the standard risk assessment matrix criteria for unencrypted emails pertains to VA email and no matrices criteria specifically applies to text messaging.[63] The review included an analysis of the specific patient sensitive personal information, how the data was stored, the ease of access and the degree of protection for the unencrypted personal emails, Cloud storage, Word documents, personal cell phone texts, and the length of time sensitive personal information was kept in an unprotected status. OIG staff concluded that, although the review found no evidence

[63] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

that unauthorized persons accessed patient sensitive personal information, the GI provider and facility staff increased the risk and possibility that sensitive personal information for the 133 patients could have been disclosed or accessed by unauthorized persons.

5. Other Finding: 2019 VA Handbook 6500.2

Although VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information* was revised March 29, 2019, the OIG identified that the handbook does not address issues identified in this report. The handbook does not include a process and guidance to address sensitive personal information incidents and events such as the use of personal email systems to transfer and store patient sensitive information and texting with personal cell phones. With this gap in policy, sensitive personal information could be disclosed or accessed by unauthorized persons.[64]

6. Other Finding: Risk of Sensitive Personal Information Disclosure with Logbooks

Although generally prohibited by the VHA policy, the facility staff used paper logbooks, with patient sensitive personal information.

VHA policy states that "VHA employees may maintain required electronic log books with appropriate safeguards in place;" however, physical/paper logbooks are not allowed "unless there is a mandatory regulation that requires the physical log book."[65]

Facility policy for the creation of logbooks expressly stated that logbooks containing sensitive personal information will only be stored electronically on authorized VA systems except when physical logbooks have been approved by the Facility Director and when there was a compelling business need and the business need is supported by a VHA Directive or some legal authority. However, the policy did not reference VHA privacy policy on logbooks, which requires a mandatory regulation for a physical logbook.[66]

A member of the GI laboratory staff stated that two physical logbooks with sensitive personal information are kept on patients using testing equipment that is taken home. The logbooks are used by technicians and nurses working in the unit.

The OIG found no mandatory regulation to keep this type of equipment logbook with sensitive personal information and that facility policy and practice to use these logbooks did not meet the intent of VHA policy to only use physical logbooks when there is a "mandatory regulation that requires the physical log book."[67]

[64] VA Handbook 6500.2, 2016; VA Handbook 6500.2, 2019.

[65] VHA Directive 1605.01.

[66] Facility Policy 00-57, *Creation and Use of Logbooks,* March 5, 2018.

[67] VHA Directive 1605.01.

Conclusion

The facility HRM lacked the ability to interface with the EHR beginning in 2013 when the VA upgraded from Windows XP operating system to Windows 7. The facility HRM remained operational and the decision was made to continue to use the medical device even though it could not interface with the EHR. Based on this decision, the GI provider developed and implemented two workarounds that were not in accordance with the VA's Rules of Behavior and policy. These workarounds included the use of the personal computer, personal emails, a non-VA unencrypted flash drive, and the Cloud.

Eight of 11 additional medical devices also lacked the ability to interface with the EHR; however, the providers and staff using these medical devices in the GI laboratory, neurology, and pulmonary/sleep laboratory developed workarounds to ensure the secure transfer of data, results, and images from the medical devices to the EHRs.

Biomed and IT initially assisted the GI provider with resolving the facility HRM's inability to interface with the EHR. However, according to the GI provider, Biomed, and IT did not address additional interface issues and the GI provider developed workarounds to transfer patient information from the facility HRM to the EHR. The OIG could not confirm the GI provider's statements as there was no documentation of the requests and the identified Biomed staff member no longer worked for the facility. The OIG noted a lack of discussion or at least documentation between the GI provider, Biomed, and IT on how the GI provider would transfer data from the facility HRM to the EHR.

The OIG established that the providers and staff in GI laboratory, neurology, and pulmonary/sleep laboratory developed their own workarounds to transfer information into the patient's EHR when their medical devices could not interface with the EHR. The OIG did not find that these providers or staff relied on Biomed or IT for assistance with developing their workarounds.

Although staff were aware of the importance to secure patients' sensitive personal information, one facility staff member sent unencrypted emails, and staff sent text messages and text pages utilizing SPOK. The OIG identified that 99 percent of emails sent from the GI provider's personal email account and 91.7 percent of text messages between the GI provider and staff contained patients' sensitive personal information.

The OIG concluded that outpatient clinic and lab staff and providers preferred mode of communication was the telephone, but if sending a text message with a personal cell phone, the nursing staff reported that the text messages stated, "call me," "patient here," and "come to clinic." Inpatient nursing and unit staff preferred mode of communication was SPOK. Although the OIG found that inpatient nursing staff sent patients' sensitive personal information through the non-secured SPOK system, the OIG believes that it is plausible that the nursing staff either overlooked the warning, or possibly assumed that because they could access the SPOK system through the facility's intranet site, then it was a secure system.

The ISSO and the privacy officer had a difference of opinion when asked what constituted sensitive personal information. For example, when asked if a text message containing a patient's first initial of the last name and the last four of the social security number (for example A1234) was appropriate, one agreed that that information was acceptable to use while the other viewed it as sensitive personal information and should not be sent over a text message. The ISSO advises staff to use the least amount of information necessary to conduct business and to encrypt messages that contain sensitive personal information and stated advising that staff should use their own judgment when making that determination.

Although the ISSO entered and tracked a ticket in PSET system for missing/stolen equipment, the OIG found that the ticket information appeared limited and incomplete. The NSOC provided no guidance to the facility on this ticket.

The OIG identified 133 patients mentioned in the GI provider's personal emails and text messages. The OIG requested that the Facility Director consider what, if any actions need to be taken to address this incident. The Facility Director, through the privacy officer, entered a new PSET system report/ticket for mishandled information with additional data. However, based on the information given to the OIG staff by the Facility Director, the data did not include the GI provider's personal email or staff texting issues. The data breach response service did not consider the information on the ticket a breach as no evidence was provided that the sensitive personal information had been disclosed to unauthorized persons. Therefore, unless additional information was provided to establish a breach had occurred, the 133 identified patients would not be offered credit monitoring.

Although the unencrypted personal emails and text messages did not meet the VA matrix criteria for a breach, OIG concluded that patient sensitive personal information was at risk for disclosure to outside sources. A complete/full risk assessment would have shown a possibility of disclosure based on the ease to obtain the information and the length of time the unencrypted information remained on an unprotected site.

In addition, although the VA handbook that addressed guidance to sensitive personal information incidents and events was revised March 29, 2019, the OIG identified that the handbook does not address issues identified in this report.

The OIG also identified that facility staff were using two physical logbooks containing patients' sensitive personal information that tracked testing equipment taken home by patients. The use of physical logbooks violates VHA policy.

Recommendations 1–6

1. The Tibor Rubin VA Medical Center Director reviews the communication processes between employees and Biomedical Engineering and Information Technology departments regarding disclosure of patient sensitive information when interface issues exist and takes necessary actions to improve this communication.

2. The Tibor Rubin VA Medical Center Director ensures that facility healthcare staff can identify which patient information or combination of patient information is considered protected from disclosure and staff transfers protected information across all communication modes, including emails and text pages, according to VA/Veterans Health Administration policy.

3. The Tibor Rubin VA Medical Center Director ensures that the Privacy Officer and the Information Systems Security Officer take necessary steps when protected patient information is compromised or possibly breached.

4. The Tibor Rubin VA Medical Center Director considers offering credit monitoring to the 133 identified patients.

5. The VA Assistant Secretary for Information and Technology reviews and adjusts the Veterans Administration Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, to include a process and guidance to address sensitive personal information incidents and events such as the use of personal email systems to transfer and store patient sensitive information and texting with personal cell phones.[68]

6. The Tibor Rubin VA Medical Center Director reviews the facility's policy and use of physical logbooks and ensures compliance with Veterans Health Administration policy.

[68] The OIG submitted the recommendation to the VA Assistant Secretary for Information and Technology; the Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer responded.

Appendix A: VA Principal Deputy Assistant Secretary Comments

Department of Veterans Affairs Memorandum

Date: July 1, 2019

From: Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer (005A)

Subj: Healthcare Inspection—Episodes of Non-Adherence to Privacy and Security Policies at the Tibor Rubin VA Medical Center, Long Beach, California

To: Director, Office of Healthcare Inspections, (54HL004)
Director, GAO/OIG Accountability Liaison (GOAL) Office (VHA 10EG GOAL Action)

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, *"Alleged Violations of Patient Information Privacy and Security Policies."* The Office of Information and Technology concurs with OIG's finding and submits the attached written comments for recommendation 5. If you have any questions, contact me at (202) 461-6910 or have a member of your staff contact Martha Orr, Deputy Chief Information Officer for Quality, Performance and Risk at (202) 461-5139.

(Original signed by:)

Dominic Cussatt
PDUSH

Comments to OIG's Report

Recommendation 5

The VA Assistant Secretary for Information and Technology reviews and adjusts the Veterans Administration Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, to include a process and guidance to address sensitive personal information incidents and events such as the use of personal email systems to transfer and store patient sensitive information and texting with personal cell phones.

Concur. The Office of Information and Technology (OIT) concurs with OIG's recommendation that VA policy and procedures should address sensitive personal information incidents and events, including the use of personal email systems and personally-owned devices to conduct VA business involving VA sensitive information.

Target date for completion: OIT requests closure of the recommendation based on the information provided below.

VA Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer Comments

OIT believes that VA policies, procedures, and guidance already in place fully address the recommendation. The most common types of privacy events are included in VA Handbook 6500.2 as specifically identified exclusions. VA always strives to incorporate emergent and trending events in future updates, however, it would be impractical to specifically address each type of potential privacy and security event by name and method in each iteration of VA policy. In addition, existing policy is in place addressing the use of personal email, mobile devices, and personally-owned devices to conduct VA business involving VA sensitive information – including VA Handbook 6500, VA Rules of Behavior, VA cybersecurity policies, and Standard Operating Procedures (SOP).

After a thorough review of this report and the subsequent recommendations, as well as the noted Privacy and Security Event Tracking System (PSETS) events, OIT believes that the OIT data breach response service (DBRS), in conjunction with the facility Privacy Officer (PO) and Information System Security Officer (ISSO), took appropriate actions as required in VA policy. A standard risk assessment was performed, and the required mitigation steps were executed in accordance with VA policy. While all methods are not failproof, the continued review of each event on a case by case basis will ensure proper mitigation for future events.

OIG Comment

The OIG considers this recommendation open to allow time for the submission of documentation to support closure.

Appendix B: VISN Director Comments

Department of Veterans Affairs Memorandum

Date: June 11, 2019

From: Director, Desert Pacific Healthcare Network (10N22)

Subj: Healthcare Inspection—Episodes of Non-Adherence to Privacy and Security Policies at the Tibor Rubin VA Medical Center, Long Beach, California

To: Director, Office of Healthcare Inspections, (54HL004)
Director, GAO/OIG Accountability Liaison (GOAL) Office (VHA 10EG GOAL Action)

I have reviewed and concur with the findings and recommendations in the OIG report entitled Healthcare Inspection - Episodes of Non-Adherence to Privacy and Security Policies at the Tibor Rubin VA Medical Center, Long Beach, California.

If you have any questions, contact me at (562) 826-5963. Thank you.

(Original signed by:)

Michael W. Fisher
VISN 22 Network Director

Appendix C: Facility Director Comments

Department of Veterans Affairs Memorandum

Date: June 11, 2019

From: Director, Tibor Rubin VA Medical Center (600)

Subj: Healthcare Inspection—Episodes of Non-Adherence to Privacy and Security Policies at the Tibor Rubin VA Medical Center, Long Beach, California

To: Director, Desert Pacific Healthcare Network (VISN 22)

Please find the attached response to the VA Office of Inspector General’s report on Episodes of Non-Adherence to Privacy and Security Policies at the Tibor Rubin VA Medical Center.

We concur with all recommendations.

(Original signed by:)

Walt C. Dannenberg, FACHE
Medical Center Director

Comments to OIG's Report

Recommendation 1

The Tibor Rubin VA Medical Center Director reviews the communication processes between employees and Biomedical Engineering and Information Technology departments regarding disclosure of patient sensitive information when interface issues exist and takes necessary actions to improve this communication.

Concur.

Target date for completion: September 30, 2019

Director Comments

The Tibor Rubin VAMC has a process in place regarding disclosure of patient sensitive information when interface issues exist. Employees utilizing equipment which interfaces with Biomedical Engineering (Biomed) and Information Technology departments will immediately notify Biomed of the issue by placing a work order or by placing a call to Biomed, identifying the problem. Biomed will take appropriate actions to resolve the problem. Biomed will work closely with Area IT manager to resolve any network connectivity issues involving the equipment. As necessary, equipment may require temporary removal from the network to prevent any unauthorized disclosures. The Tibor Rubin VA Medical Center Director has directed the Privacy Officer to lead a Privacy and Security Stand Down. The information listed above will be included in the stand down and presentation materials will be sent to all staff.

Recommendation 2

The Tibor Rubin VA Medical Center Director ensures that facility healthcare staff can identify which patient information or combination of patient information is considered protected from disclosure and staff transfers protected information across all communication modes, including emails and text pages, according to VA/Veterans Health Administration policy.

Concur.

Target date for completion: September 30, 2019

Director Comments

The Tibor Rubin VA Medical Center Director has directed the Privacy Officer to lead a Privacy and Security Stand Down. This event will be open to all staff in person or via Skype. The presentation materials will be sent to all staff.

Recommendation 3

The Tibor Rubin VA Medical Center Director ensures that the Privacy Officer and the Information Systems Security Officer take necessary steps when protected patient information is compromised or possibly breached.

Concur.

Target date for completion: June 10, 2019

Director Comments

Response: The Privacy Officer or the Information System Security Officer will immediately submit a Privacy Security Event Tracking ticket to Cyber Security Operations Center. The Privacy and Information Systems Security Officer offices will send an email to the VHA Incident response team informing the team that a privacy breach has occurred, and the team will assemble to discuss the breach and ensure all steps have been implemented per VHA Directive 1605.01. Senior Leadership will be notified by email of the occurrence and kept informed of the actions being taken to contain the breach.

OIG Comment

The OIG considers this recommendation open to allow time for the submission of documentation to support closure

Recommendation 4

The Tibor Rubin VA Medical Center Director considers offering credit monitoring to the 133 identified patients.

Concur.

Target date for completion: October 22, 2018

Director Comments

The Tibor Rubin VA Medical Center Director requested to provide credit monitoring to the 133 identified patients and was informed by the National Data Breach Response Service that this incident did not meet the criteria of a privacy breach, and the request to provide credit monitoring was denied.

OIG Comment

The OIG considers this recommendation open to allow time for the submission of documentation to support closure

Recommendation 6

The Tibor Rubin VA Medical Center Director reviews the facility's policy and use of physical logbooks and ensures compliance with Veterans Health Administration policy.

Concur.

Target date for completion: June 14, 2019

Director Comments

The Tibor Rubin VA Medical Center Director is aware of and has reviewed the Privacy Program and Creation and Use of Log Books Health System Policies (HSPs). The Director will send out the HSPs to the Healthcare System Employees as a reminder of the importance of protecting our patient's privacy. As part of the Privacy and Security Stand Down, the HSPs will be reviewed and Log Book usage will be audited.

OIG Comment

The OIG considers this recommendation open to allow time for the submission of documentation to support closure.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Inspection Team	Elaine Kahigian, RN, JD, Director W. Iris Barber, JD Kelli Brice, MPT Joanne Wasko, LCSW
Other Contributors	Michael Bowman Elizabeth Bullock Jennifer Christensen, DPM Sheyla Desir, RN, MSN Simonette Reyes, BSN, RN

Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Assistant Secretaries
General Counsel
Director, Desert Pacific Healthcare Network (10N22)
Director, Tibor Rubin VA Medical Center (600/00)

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
U.S. Senate: Dianne Feinstein and Kamala D. Harris
U.S. House of Representatives: Nanette Barragán; Gilbert Ray Cisneros, Jr.; J. Luis Correa; Mike Levin; Alan Lowenthal; Grace Napolitano; Katie Porter; Harley Rouda; Linda Sánchez; Maxine Waters

The OIG has federal oversight authority to review the programs and operations of VA medical facilities. OIG inspectors review available evidence to determine whether reported concerns or allegations are valid within a specified scope and methodology of a healthcare inspection and, if so, to make recommendations to VA leadership on patient care issues. Findings and recommendations do not define a standard of care or establish legal liability.

OIG reports are available at www.va.gov/oig.