Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

Two Indian Health Service Hospitals Had System Security and Physical Controls for Prescription Drug and Opioid Dispensing but Could Still Improve Controls

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

November 2017
A-18-16-30540

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG’s internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Report in Brief
Date: November 2017
Report No. A-18-16-30540

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Why OIG Did This Review

We conducted this review to assess the Indian Health Service's (IHS) physical and information technology controls over prescription drugs such as opioids and to identify measures that could prevent drug diversions.

HHS has recognized the escalating abuse of opioid drugs in our society. Among HHS operating divisions, the Centers for Disease Control and Prevention, National Institutes for Health, and IHS play key roles in HHS's programmatic response to the nation-wide epidemic.

IHS is responsible for implementing appropriate controls within IHS to protect prescription drugs, including opioids; IHS is also responsible for the security of related beneficiaries' personal health information in accordance with Federal security requirements.

Our objective was to determine whether IHS implemented federally required physical and information technology systems controls that would help to ensure prescription drugs (specifically opioids) are dispensed appropriately.

How We Conducted This Review

We reviewed IHS's policies and procedures, reviewed physical security controls, interviewed staff, and used vulnerability scanning software to determine whether security related vulnerabilities existed on the Personal Health Record website.

Two Indian Health Service Hospitals Had System Security and Physical Controls for Prescription Drug and Opioid Dispensing but Could Still Improve Controls

What OIG Found

Although IHS had increased system security and physical controls surrounding prescription drug and opioid disbursements, IHS did not adequately implement information technology security controls to address risks related to health information and patient safety.

Specifically, we found that: two IHS hospitals had system security and physical controls for prescription drug and opioid dispensing; an IHS hospital lacked an adequate continuity of operations program and disaster recovery plan; two IHS hospitals did not have adequate logical access control procedures; two IHS hospitals lacked adequate information technology risk assessments; and, one IHS hospital lacked adequate flaw remediation and vulnerability management procedures.

What OIG Recommends and IHS Comments

We recommend that IHS:

- take immediate action to assess all IHS facilities and ensure each facility has a tested and viable continuity of operations program to respond to and recover from a range of disasters;
- test all backup mechanisms at all IHS hospitals to ensure patient information is fully recoverable and implement an effective continuity of operations program and disaster recovery plan and procedures in accordance with Federal requirements;
- develop and implement logical access control procedures to ensure compliance with the principle of least privilege and conduct privileged-based access reviews to remove unnecessary access to the Resource Patient Management System;
- perform information security risk assessments at all IHS hospitals in accordance with Federal requirements;
- identify all IHS hospitals with unsupported equipment and implement a system development life cycle plan to ensure hardware and software replacement prior to end-of-life; and
- determine if local IHS hospital system administrators are adequately trained to ensure compliance with all flaw remediation and vulnerability management procedures and, if not, develop a training program.

IHS concurred with all of our recommendations and described the actions it had taken and plans to take to implement them.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181630540.asp.

TABLE OF CONTENTS

APPENDICES

INTRODUCTION

WHY WE DID THIS REVIEW

We conducted this review to assess the Indian Health Service's (IHS) physical and information technology (IT) controls over prescription drugs such as opioids and to identify measures that could prevent drug diversions. The U.S. Department of Health and Human Services (HHS) has recognized the escalating abuse of opioid drugs in our society. Among HHS operating divisions, the Centers for Disease Control and Prevention (CDC), National Institutes for Health (NIH), and Indian Health Service (IHS) play key roles in HHS's programmatic response to the nationwide epidemic. OIG identified curbing the abuse and misuse of controlled and non-controlled drugs in Medicare Part D and Medicaid as one of HHS's top management challenges. In July 2017 the OIG Office of Evaluations published a data brief, "Opioids in Medicare Park D: Concerns about Extreme Use and Questionable Prescribing."[1]

Drug diversions[2] are a serious contributing factor to the opioid crises. In June 2013, the HHS Office of Inspector General (OIG) spotlighted[3] the impact of potential opioid abuse on HHS programs and beneficiaries. In 2011, IHS experienced a diversion at a pharmacy that resulted in more than 48,000 stolen opioid pills and the arrest and felony conviction of five individuals. OIG investigators found that the diversion resulted from inadequate physical controls and internal controls in the pharmacy and hospital.

To inform our understanding of the control environments for the management of opioids within IHS facilities, we requested opioid purchase information for fiscal years (FYs) 2013 through 2016 from the primary vendor for all IHS sites (tribal and Federal).[4] IHS provided the following data:

[1] Available online at https://oig.hhs.gov/oei/reports/oei-02-17-00250.pdf

[2] "Drug diversion" is the illegal distribution or abuse of prescription drugs or their use for unintended purposes. Drug diversion can result in drug addictions, overdoses, drug-related emergency room visits, and death and has contributed to a significant increase in substance abuse treatment admissions.

[3] Available online at https://oig.hhs.gov/newsroom/spotlight/2013/diversion.asp.

[4] IHS officials stated that using the purchase information was the most reliable way to approximate the opioids within IHS facilities.

Table: IHS Opioid Purchase Information for FYs 2013 through 2016

FY/Total	Opioids[5]	IHS User Population[6]
2013	50,980,890	1,576,629
2014	49,336,116	1,598,385
2015	45,804,877	1,613,450
2016	41,737,804	1,626,826
Total	**187,859,687**	**6,415,290**

The total number of opioids purchased for FYs 2013 through 2016 was 187,859,687 opioids. The user (patient) population during that same time period was 6,415,290.[7] Our audit scope did not include a detailed analysis of IHS opioid prescribing practices. Therefore we did not examine pharmaceutical details (e.g., types of opioids) or prescribing practices, such as morphine equivalents (potency) across all facilities, implementation of Centers for Disease Control and Prevention opioid prescribing guidelines[8], beneficiary characteristics (including diagnoses), the total number of beneficiaries who were prescribed opioids, or the total number of doses that the 187 million purchased opioid figure represented. We are planning future work to examine IHS opioid prescribing practices.

We judgmentally selected and visited two IHS facilities: Quentin N. Burdick Memorial Hospital (Burdick Memorial) in Belcourt, North Dakota, and Blackfeet Community Hospital (Blackfeet Hospital) in Browning, Montana. We selected Burdick Memorial because it was the site of the drug diversion referenced above. We selected Blackfeet Hospital because it was located in a different IHS administrative area, and according to IHS officials, the prescription drugs dispensed at Blackfeet Hospital had a higher morphine equivalent (i.e., opioid potency) when compared with Burdick Memorial. (See Background, "Indian Health Service Management Structure.") According to IHS, for FYs 2013 through 2016, Burdick Memorial purchased 3,400,227 opioids and had a user population of 55,568. Blackfeet Hospital purchased 1,238,562 opioids and had a user population of 46,178.

[5] Throughout this report, we use the term "opioids" to reflect the unit of measurement IHS used when reporting purchase information to OIG based on our data request. It does not necessarily equate to the number of doses purchased, prescribed, or dispensed.

[6] IHS user population is defined as the number of Indian registrants residing within a service delivery area with at least one face-to-face, direct or contract, inpatient stay, ambulatory care visit, or dental visit during the prior three FYs.

[7] The 6,415,290 represents the total IHS user population from FYs 2013 through 2016. Some users are counted in multiple years (e.g., the same IHS user (patient) maybe counted in FYs 2014 and 2015). The population data we obtained includes everyone from infants to the elderly.

[8] CDC, *Guideline for Prescribing Opioids for Chronic Pain – United States, 2016.* Available online at https://www.cdc.gov/mmwr/volumes/65/rr/rr6501e1.htm. Accessed on March 15, 2017.

IT systems play an important role in the internal controls to prevent drug diversion. Data integrity, access controls, and the underlying network that supports IT systems are critical components in ensuring prescriptions (including opioids) are filled in accordance with doctors' orders.

OBJECTIVE

Our objective was to determine whether the IHS has implemented federally required physical and IT systems controls that would help to ensure prescription drugs (specifically opioids) are dispensed appropriately.

BACKGROUND

Opioid Epidemic and HHS's Response

Federal agencies within the Government have been working to curb the nation-wide opioid abuse epidemic that causes 91 deaths per day in the United States.[9] In August 2015, the U.S. Surgeon General took the unprecedented step of writing a letter to all clinicians requesting their help to solve the opioid epidemic.[10]

> Young adults (age 18 to 25) are the biggest abusers of prescription (Rx) opioid pain relievers, ADHD stimulants, and anti-anxiety drugs. They do it for all kinds of reasons, including to get high or because they think prescription stimulants will help them study better. But [prescription drug] abuse is dangerous. In 2014, more than 1,700 young adults died from prescription drug (mainly opioid) overdoses—more than died from overdoses of any other drug, including heroin and cocaine combined—and many more needed emergency treatment.[11]

In March 2016, the IHS Chief Medical Officer emailed all IHS employees telling them that appropriate prescribing of opioid medications and management of chronic pain were of critical importance within IHS. The email included a link to the CDC guidance on opioid prescribing practices. In July 2016, Congress passed the Comprehensive Addiction and Recovery Act of 2016 to combat the heroin and opioid abuse crisis.[12] And on April 19, 2017, the HHS Secretary

[9] CDC, *Drug Overdose Deaths in the United States Continue To Increase in 2015.* Available online at https://www.cdc.gov/drugoverdose/epidemic/index.html. Accessed on March 15, 2017.

[10] United States Surgeon General, Vivek H. Murthy, M. D., M.B.A. Available online at http://i2.cdn.turner.com/cnn/2016/images/08/25/sg.opioid.letter.pdf. Accessed on March 15, 2017.

[11] NIH. Available online at https://www.drugabuse.gov/related-topics/trends-statistics/infographics/abuse-prescription-rx-drugs-affects-young-adults-most. Accessed on March 15, 2017.

[12] P.L. No. 114-198. Available online at https://www.congress.gov/bill/114th-congress/senate-bill/524/text. Accessed on March 15, 2017.

announced that HHS would distribute grants totaling $485 million to all 50 States to combat opioid addiction.[13] The President signed an Executive Order on March 29, 2017 establishing the President's Commission on Combating Drug Addiction and the Opioid Crisis chaired by the Governor of New Jersey. [14]

Within HHS, CDC and NIH have taken steps to ensure the public is aware of the dangers associated with chronic opioid use. IHS is responsible for implementing appropriate controls within IHS to protect prescription drugs, including opioids; IHS is also responsible for the security of related beneficiaries' personal health information in accordance with Federal security requirements.

Indian Health Service

IHS is responsible for providing Federal health services to American Indians and Alaska Natives (AI/ANs) and has an annual appropriation of $4.8 billion. According to its website, IHS's mission is "to raise the physical, mental, social, and spiritual health of American Indians and Alaska Natives to the highest level." In partnership with the 567 federally recognized tribes, IHS provides free primary and preventive health care services to approximately 2.2 million AI/ANs living in the United States. Health disparities and inadequate health care services for AI/ANs have been a subject of concern for the Federal Government for almost a century.

Indian Health Service Management Structure

IHS has a management structure that is separated into two major categories: Headquarters office and 12 Area offices, each of which supports a specific region of the United States. IHS headquarters issues guidance for Area offices and local IHS hospitals.

The Great Plains Area office in Aberdeen, South Dakota, works in conjunction with its 19 IHS service units to provide health care to approximately 130,000 AI/ANs located in North Dakota, South Dakota, Nebraska, and Iowa. The Great Plains Area office's service units include seven hospitals, including Burdick Memorial, eight health centers, and several smaller health stations and satellite clinics.

The Billings Area Office in Billings, Montana, provides health care to approximately 70,000 AI/ANs in Montana and Wyoming through six service units, one of which includes the Blackfeet Hospital, two self-governance service units, and five urban programs.

[13] HHS, Trump Administration Awards Grants to States to Combat Opioid Crisis. Available online at https://www.hhs.gov/about/news/2017/04/19/trump-administration-awards-grants-states-combat-opioid-crisis.html. Accessed on August 31, 2017.

[14] White House. Available online at https://www.whitehouse.gov/ondcp/presidents-commission. Accessed on August 31, 2017.

The Two Indian Health Service Health Care Facilities

Burdick Memorial has 27 beds and 11 physicians who provide both inpatient and outpatient services. In addition to inpatient care, the hospital has a pharmacy and provides general surgery, podiatry, ear-nose-throat surgery, obstetrics, and Computed Axial Tomography scans.

Blackfeet Hospital has 28 beds and 13 physicians who provide services in family practice and emergency room care. The facility also provides physical therapy, has a diabetes program, and a pharmacy.

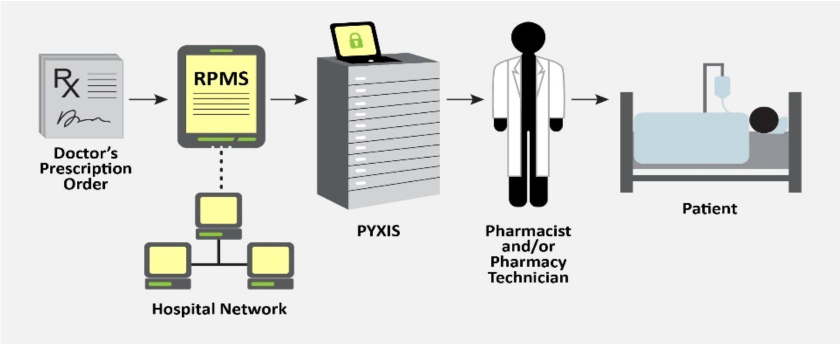
Resource and Patient Management System

The IHS electronic health record system, the Resource and Patient Management System (RPMS), is an automated information system consisting of more than 60 integrated software applications. The RPMS is designed to operate on computers located at more than 400 IHS, tribal, urban Indian health, and public health nursing sites or facilities. The IHS Office of Information Technology is primarily responsible for the development and distribution of RPMS to all IHS locations. Implementation of specific RPMS functions (e.g., assigning system privileges) is the responsibility of the individual Area office, service unit, hospital, or clinic.

Pyxis

The pharmacies we visited had implemented an automatic drug dispensing system called Pyxis (see Figure 1). The manufacturer describes Pyxis as an "automated medication dispensing system [that] supports decentralized medication management with various features for safety and efficiency. The system helps accurately dispense medication, while supporting pharmacy workflows."[15] Pyxis receives patient and prescription data via a one-way communication link from RPMS to Pyxis. Both pharmacies that we visited use Pyxis; more information about this process can be found in subsequent sections of this report.

Figure 1: Prescription Drug Dispensing Process at Burdick Memorial and Blackfeet Hospital


Rx
Doctor's Prescription Order
RPMS
Hospital Network
PYXIS
Pharmacist and/or Pharmacy Technician
Patient

[15] http://www.bd.com/en-us/offerings/capabilities/medication-and-supply-management/medication-and-supply-management-technologies/pyxis-medication-technologies/pyxis-medstation-system. Accessed on June 30, 2017.

FEDERAL REQUIREMENTS

To determine whether IHS had implemented federally required IT systems and physical security controls that could help to ensure prescription drugs, such as opioids, were dispensed appropriately, we used Federal requirements from the Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*; NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; and NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments* (Appendix A).

IHS requirements relating to prescription drugs are the *Indian Health Manual,* section 8-12.1, which makes IHS responsible for securing information that it collects, records, transmits, and uses in the performance of its mission, and the *Indian Health Manual,* section 3-7.3D (xii)(c)(i), which states that Schedule II drugs should be stored in a substantially constructed locked cabinet, safe, or drawer.

HOW WE CONDUCTED THIS REVIEW

We reviewed IHS's information system general and physical controls as they relate to electronic health care and pharmaceutical access controls at two IHS-operated hospitals: Burdick Memorial and Blackfeet Hospital. To accomplish our objective, we used appropriate procedures from applicable Federal regulations and guidance. We reviewed policies and procedures, interviewed staff at IHS headquarters and the two IHS hospitals, and reviewed supporting documentation. To identify potential security-related configuration vulnerabilities on IHS's Personal Health Record (PHR) website,[16] we used audit software-scanning programs.

We limited our review to IHS's implementation of certain information system and physical controls supporting the dispensing of prescription drugs. We did not review IHS's overall internal controls. Our observations are specific to the two IHS-operated facilitates that we visited, Burdick Memorial and Blackfeet Hospital. At these two hospitals we focused on the effect pharmacy operations' and IT vulnerabilities could have on possible drug diversions and patient data and care. We do not opine on the controls across IHS; however, we have included recommendations for IHS to determine if some of the issues we identified are systemic in IHS.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We shared with IHS

[16] Available online at https://phr.ihs.gov; the PHR website is the patient portal for IHS patients.

information about our vulnerability scan findings immediately after we finished the scans and informed IHS about other preliminary findings before issuing our draft report.

We conducted our fieldwork at Burdick Memorial from October 31 through November 4, 2016; Blackfeet Hospital from November 14 through 18, 2016; and IHS Headquarters in Rockville, Maryland, from January 23 through 27, 2017.

Appendix A contains specific Federal requirements for protecting health information. Appendix B contains the details of our audit scope and methodology. Appendix C contains photographic examples of the physical environment at Burdick Memorial and Blackfeet Hospital.

FINDINGS

To help ensure prescription drugs such as opioids are secured and available for appropriate dispensing, IHS had some system and physical controls at the two hospitals we visited. However, IHS did not adequately implement IT security controls to protect health information and patient safety at those hospitals. This occurred because IHS's IT risk assessments did not effectively assess and mitigate information security risk. As a result, IHS hospital operations and delivery of patient care could be significantly affected.

Specifically, we identified weaknesses in the following control areas:

- physical security,
- continuity of operations program and disaster recovery plan,
- logical access,
- information technology risk assessments, and
- flaw remediation and vulnerability management.

In addition, our vulnerability scan of the PHR website identified 25 vulnerabilities, which the tool we used (WebInspect[17]) classified as high (1 vulnerability), medium (2 vulnerabilities), and low (22 vulnerabilities). We did not identify any vulnerabilities WebInspect defined as critical. While our scan identified a small number of vulnerabilities on the PHR website, the results indicated that IHS had patched and monitored most of the known vulnerabilities. However, IHS continued to have network vulnerabilities because local system administrators were not properly trained.

[17] WebInspect describes the relative severity of a vulnerability as follows: critical, a vulnerability wherein an attacker might have the ability to execute commands on the server or retrieve and modify information; high, the ability to view source code, files, and messages; medium, non-HTML errors or concerning issues that could be sensitive; and low, interesting issues or issues that could potentially become higher-ranking ones.

TWO IHS HOSPITALS HAD SYSTEM SECURITY AND PHYSICAL CONTROLS FOR PRESCRIPTION DRUG AND OPIOID DISPENSING BUT COULD STILL IMPROVE CONTROLS

Some System Security and Physical Controls Were Implemented

Burdick Memorial and Blackfeet Hospital had system and physical controls to ensure prescription drugs and pharmacy information were protected, thus lessening the chance that prescriptions could be illegally diverted.

The *Indian Health Manual,* section 3-7.3D (xii)(c)(i), states: Schedule II drugs should be stored in a substantially constructed locked cabinet, safe or drawer. For other Scheduled drugs, it is strongly suggested that only a small working stock be dispersed among regular stock with the remainder securely stored under lock and key.

Both hospitals implemented a system called Pyxis (Appendix C, photographs 1, 2, and 3), which was used in combination with physical controls (e.g., cameras and badge access) to ensure prescription drugs and controlled substances were not illegally diverted from the pharmacies and hospitals. Pyxis is an automated dispensing medication system for all drugs, including Scheduled drugs. Pyxis controls include locked drawers, restrictions to medication dispensing based on physician orders, and access restrictions via biometric technology (e.g., fingerprints). Once the drug to be dispensed has been selected, the system automatically counts the pills and restricts access to other drugs by using secure compartments. Overall, Pyxis is designed to ensure safe, accurate, and efficient medication dispensing.

As noted above, Burdick Memorial had a drug diversion in 2011 that resulted in more than 48,000 stolen opioid pills and the conviction of five individuals. The drug diversion resulted from inadequate physical controls and internal controls over the pharmacy inventory. At the time of the incident, the OIG Office of Investigations recommended that Burdick Memorial improve physical controls to mitigate future drug diversion risk. Based on those recommendations, Burdick Memorial pharmaceutical and Great Plains Area office staff implemented a robust program for controlling prescription drug dispensing. Burdick Memorial enhanced physical controls, such as installing a locked cage with cameras where controlled substances were maintained (Appendix C, photograph 4), cameras throughout the hospital and in areas where patients pick up their prescriptions (Appendix C, photograph 5), and a badge and personal identification number (PIN) code access system to the pharmacy (Appendix C, photograph 6). As a result of the improvements, we did not identify weaknesses related to the physical and system controls in place at Burdick Memorial.

Blackfeet Hospital also implemented Pyxis (Appendix C, photograph 3) and had similar physical controls in place as Burdick Memorial.

Blackfeet Hospital's Controls Over Pharmacy Access Could Be Improved

NIST SP 800-53, Appendix F, PE-2, states that an organization ". . . issues authorization credentials for facility access . . . [and] enforces physical access authorizations by verifying individual access authorizations before granting access to the facility." This standard is for physical access to areas where IT systems such as Pyxis are located.

The *Indian Health Manual,* section 3-7.3D (xii)(c)(i), states: Schedule II drugs should be stored in a substantially constructed locked, cabinet, safe or drawer. For other Scheduled drugs, it is strongly suggested that only a small working stock be dispersed among regular stock with the remainder securely stored under lock and key.

Blackfeet Hospital could improve controls at entry points to sensitive areas of the hospital to protect both the Pyxis system and pharmacy inventory from unauthorized access. Access to Blackfeet Hospital's pharmacy (Appendix C, photograph 7) where regular drug stock were stored was controlled by assigning one PIN to a group of people. Pharmacists used one shared PIN and pharmacy technicians used another to enter the pharmacy. This occurred because Blackfeet Hospital did not sufficiently assess the risk associated with shared PINs. Without unique PINs, Blackfeet Hospital management could not prevent access by unauthorized individuals or identify who had accessed the pharmacy area. Had Scheduled drugs been stolen or if an individual obtained unauthorized physical access to the Pyxis system, security officials would have had greater difficulty determining who had entered the area at a given time.

BURDICK MEMORIAL LACKED AN ADEQUATE CONTINUITY OF OPERATIONS PROGRAM AND DISASTER RECOVERY PLAN

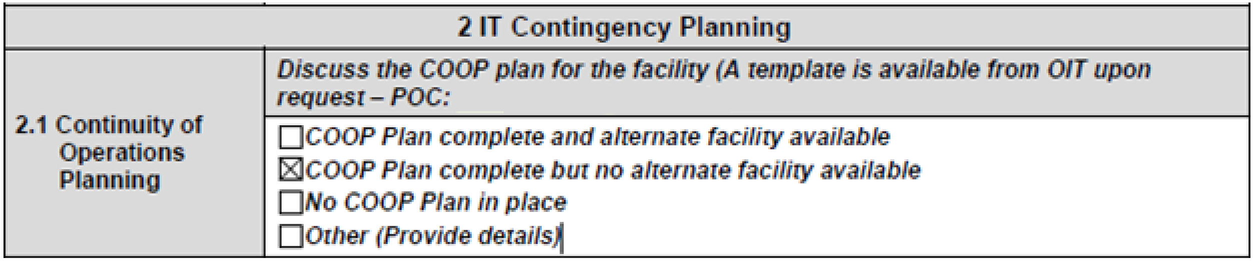
The *Indian Health Manual*, section 8-12.1H(2)(b), states that management officials shall develop and maintain contingency plans that describe the resources and procedures to be used for maintaining the continuity of applications critical to the mission of the IHS in the event of a disaster, and each contingency plan shall be tested at least once a year.

NIST SP 800-34, Revision 1, ES-1, requires organizations to: 1) create contingency strategies, thorough recovery strategies to ensure that the system may be recovered quickly and effectively following a disruption; 2) develop an information system contingency plan, which should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements; and 3) ensure plan testing, training, and exercises, testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

Burdick Memorial had an ineffective continuity of operations program and disaster recovery plan. The IHS decentralized setup required each hospital to do its own continuity of operations and disaster recovery planning until planned nation-wide shadow backups[18] were in place. Burdick Memorial relied on an archaic backup tape process and did not have a hot, warm, or cold site to host an effective continuity of operations program and disaster recovery plan.[19] After our site visit concluded but before we issued our report, IHS informed us that its Area offices conducted shadow backups of its hospitals; however, the Great Plains Area office that services Burdick Memorial had not conducted tests of those backups to ensure the integrity and availability of patient information.

Significantly, Burdick Memorial's risk assessment identified the lack of a disaster recovery site as a risk (Figure 2); however, the appropriate risk mitigation did not take place. (See the finding below "IHS Hospitals Did Not Have Adequate Information Technology Risk Assessments.")

Figure 2: Excerpt From Burdick Memorial's Risk Assessment[20]



2 IT Contingency Planning	
2.1 Continuity of Operations Planning	*Discuss the COOP plan for the facility (A template is available from OIT upon request – POC:*
	□COOP Plan complete and alternate facility available *☒COOP Plan complete but no alternate facility available* *□No COOP Plan in place* *□Other (Provide details)*

Burdick Memorial officials could not provide us clear guidance on how the hospital would retrieve patient medical records stored on damaged hardware, such as the server rack, or untested back-up tapes stored in the same area of the hospital as the server rack. As an example, if Burdick Memorial's server rack (Appendix C, photograph 8) were destroyed (e.g., through fire or water damage) or if there were a catastrophic IT failure, according to Burdick Memorial officials the hospital would continue to function by going "back to pen and paper." Burdick Memorial staff informed us that they had not tested their pen-and-paper solution. If the server rack at Burdick Memorial were inoperable, entire hospital operations could come to a halt and significantly affect patient safety and care.

Without an alternative facility or a tested backup plan, Burdick Memorial was not prepared to respond to or recover from a disaster, whether natural, manmade, or IT (e.g., ransomware). Lack of an effective contingency plan could have had a devastating effect on access to personal

[18] Shadow back-ups provide periodic snapshots of data stored at off-site locations.

[19] Hot sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel to support information system recovery activities. Warm sites are partially equipped spaces that contain some or all of the system hardware, software, telecommunications, and power sources to support information system recovery activities. Cold sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.

[20] COOP: contingency of operations plan, OIT: Office of Information Technology, POC: point of contact.

health information and prescription dispensing.[21] If prescription drug records were lost and could not be recovered, the absence of accurate information would put patient safety at risk and make Burdick Memorial's pharmacy vulnerable to inappropriate prescribing and possible drug diversion by individuals fraudulently claiming to have had prescriptions for opioids.

IHS LACKED ADEQUATE LOGICAL ACCESS CONTROL PROCEDURES AT TWO HOSPITALS AND MAY NOT HAVE HAD THEM AT OTHER HOSPITALS

NIST SP 800-53, Revision 4, AC-6, states that an organization must employ the principle of least privilege, allowing authorized access only for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Allowing unnecessary access could create opportunities for drug diversion by individuals who intended to misuse the electronic access.

The *Indian Health Manual,* section 8-19.1D, states it is the policy of the IHS that each IT user will be authorized the most restrictive set of privileges or access needed for performing authorized tasks. All elevated system privilege accounts must be controlled and limited to Office of Information Technology (OIT) support personnel, Area Information Systems Coordinators (ISC), or their designated alternates.

IHS did not have adequate logical access control procedures for RPMS access reviews at the two hospitals we reviewed because the reviews did not require supervisors to verify specific RPMS privileges (e.g., read, write, delete, and modify). The procedures and reviews had not implemented role-based access controls according to the principle of least privilege. Because the flawed access reviews at the two hospitals were mirrored across other IHS-operated hospitals, the current access review process should be reviewed throughout IHS.

An example of this problem is that Burdick Memorial administrators discovered an incident where someone with "delete" privileges deleted months of accounts-receivable data. The Great Plains Area office investigated the incident but could not determine who deleted the data because IHS had not implemented role-based access controls according to the principle of least privilege. That would have restricted the number of users with the capability to delete accounts-receivable data. Also, according to IHS officials, the associated computer logs were overwritten for capacity reasons and backup tapes did not provide the necessary data for IHS to determine who deleted the records. IHS officials informed us that they are still trying to recover data from this incident that occurred approximately 4 years ago.

[21] On November 16, 2016, CMS promulgated regulations to establish "national emergency preparedness requirements for Medicare- and Medicaid-participating [hospitals] to plan adequately for both natural and man-made disasters, and coordinate with federal, state, tribal, regional, and local emergency preparedness systems" Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers, 81 Fed. Reg. 63860 (Sept. 16, 2016) (codified at 42 C.F.R. pt. 482). The regulation attempts to increase patient safety during emergencies and establish a more coordinated response to disasters. Hospitals, including Burdick Memorial and Blackfeet Hospital, must comply with the new rule before November 16, 2017.

Without adequate logical access control procedures for RPMS, IHS cannot ensure that it can fully protect the confidently, integrity, and availability of health records and other mission critical data.

TWO IHS HOSPITALS LACKED ADEQUATE INFORMATION TECHNOLOGY RISK ASSESSMENTS

NIST 800-30 states that "risk assessments are a key part of effective risk management and facilitate decision making at all three tiers in the risk management hierarchy including the organization level, mission/business process level, and information system level." NIST 800-39, chapter 2.3.1, states: "Regardless of the governance model(s) employed, clear assignment and accountability for accepting risk is essential for effective risk management." And recently, the United States Computer Emergency Readiness Center (US-CERT) reminded users that software no longer supported by Microsoft (also known as end-of-life (EOL) software) is particularly at risk for exploitation. US-CERT recommended retiring EOL products.[22]

IHS Area offices and Headquarters personnel conducted periodic risk assessments of IHS facilities, but Burdick Memorial and Blackfeet Hospital did not have sufficient IT risk assessments, nor did the hospitals develop adequate risk mitigation plans. For example, the risk assessments at both hospitals did not incorporate the Pyxis system used for tracking and securing prescription drugs. In many instances, hospital officials accepted risk without adequate documentation or analysis; rather a blanket acceptance was granted by signing the Authorization to Operate. Failure to conduct the required risk assessments could create opportunities for drug diversion by allowing vulnerable software and other system weaknesses to remain operable.

While Burdick Memorial's previous risk assessment identified the risk of not having effective continuity of operations (Figure 2), the risk assessment did not treat the risk with the necessary emphasis and seriousness for the risk to be adequately considered. According to NIST SP 800-39, 3.3, organizations should be documenting risk management decisions at all levels of the enterprise architecture, and organizations can respond to risk by: (i) risk acceptance; (ii) risk avoidance; (iii) risk mitigation; (iv) risk sharing; (v) risk transfer; or (vi) a combination. Ultimately, Burdick Memorial management accepted the risk. The two hospitals also accepted the risks related to their lack of role-based access controls within RPMS and unsupported networking equipment. The acceptance of the RPMS risk may have contributed to the deletion of the accounts-receivable data noted above. The acceptance of risk associated with unsupported networking equipment and software approaching or past EOL left the hospitals susceptible to known vulnerabilities for which the vendor no longer provided updates and security patches.

[22] US-CERT, *Microsoft Addresses Shadow Brokers Exploits,* April 15, 2017. Available online at https://www.us-cert.gov/ncas/current-activity/2017/04/15/Microsoft-Addresses-Shadow-Brokers-Exploits-0. Accessed on April 18, 2017.

Both hospitals relied on inadequate assessments that did not thoroughly evaluate the risks associated with hospital operations. Without an adequate risk assessment, IHS hospitals could not ensure that they could identify or implement appropriate controls to reduce or eliminate risks that could affect health information and patient safety. The same template and methodology used to execute the risk assessment at Burdick Memorial and Blackfeet Hospital is used at other IHS hospitals, so it should be reviewed throughout IHS.

BURDICK MEMORIAL LACKED ADEQUATE FLAW REMEDIATION AND VULNERABILITY MANAGEMENT PROCEDURES

The *Standard Operating Procedure for IHS Enterprise Patch Management*, section 3, “Roles and Responsibility for Patch Management”, states that the enterprise IT administrators shall test all critical patches against standard supported IHS applications and operating systems within three (3) business days after vendor release and ensure availability of approved critical patches to Areas/Facilities within (5) business days of vendor release. Also, the Area Information System Security Officer (ISSO) shall test all critical security patches against local standard system configurations within three (3) business days of deployment to local site servers, and deploy all critical patches to all supported workstations and servers within ten (10) business days of availability to local site servers.

Burdick Memorial did not in a timely manner address or remediate critical vulnerabilities IHS identified during weekly scans. We selected for review 7 of the 60 critical vulnerabilities identified at Burdick Memorial in those weekly scans. We determined that 118 of approximately 250 total computers were affected by a critical vulnerability that was at least 4 years old, and 72 of the same 250 computers were affected by another critical vulnerability that was also at least 4 years old. Three months after our site visit but before we issued our report, Burdick Memorial provided documentation to support that it had partially remediated two of the seven critical vulnerabilities we selected for review and that the five remaining critical vulnerabilities were totally remediated. The vulnerabilities at Burdick Memorial were not mitigated in a timely manner because the local IT administrators for Burdick Memorial were unaware of their roles and responsibilities for remediating vulnerabilities identified during IHS network scans.

Unmitigated vulnerabilities can seriously affect hospital operations, as was demonstrated by the exploitation of the WannaCry vulnerability, which resulted from unpatched Microsoft servers. Overall, without adequate flaw remediation and vulnerability management procedures, IHS hospitals are at increased risk of compromise from known vulnerabilities, which could affect access to health information and patient safety and could create opportunities for drug diversion by unauthorized individuals manipulating electronic prescriptions to create fraudulent prescriptions or changing prescriptions to increase doses of opioids. IHS should determine if other hospitals are also not mitigating vulnerabilities in a timely manner.

WEBSITE VULNERABILITY SCAN

We performed a web application vulnerability scan on the PHR website. The results revealed 25 vulnerabilities, the severity of which the tool we used classified as high (1 vulnerability), medium (2 vulnerabilities), and low (22 vulnerabilities). The tool did not identify any critical vulnerabilities. The one high-impact vulnerability related to cross-frame scripting, and the two medium-impact vulnerabilities related to cross-frame scripting and privacy violation.[23] Our scan identified a small number of vulnerabilities for the PHR website and showed that IHS had patched and monitored scanning vulnerabilities for the website. IHS should mirror those efforts and improve its overall controls for network vulnerability scans at each hospital IHS-wide.

RECOMMENDATIONS

We recommend that IHS management implement adequate information system and physical security general controls over its protected health information surrounding prescription drugs. Specifically, we recommend that IHS:

- assign specific PINs for each employee at Blackfeet Hospital for restricted areas;
- deem a risk of the lack of continuity of operations to be unacceptable and take immediate action to assess all IHS facilities and ensure each facility has a tested and viable continuity of operations program to respond to and recover from a range of disasters;
- test all backup mechanisms at Burdick Memorial to ensure patient information is fully recoverable and implement an effective continuity of operations program and disaster recovery plan and procedures in accordance with Federal requirements;
- develop and implement logical access-control procedures to ensure compliance with the principle of least privilege and conduct periodic privilege-based access reviews to remove unnecessary access to RPMS;
- perform adequate information security risk assessments at all IHS hospitals in accordance with NIST 800-30;
- identify all hospitals with unsupported networking equipment and implement a system development life cycle plan to ensure hardware and software replacement before EOL;

[23] The site returns different results if a valid user name is entered with an invalid password versus if an invalid user name is entered with an invalid password. With this information, a hacker would know if he or she had a valid user name.

- determine if local IHS hospital system administrators are adequately trained to ensure compliance with all flaw remediation and vulnerability management procedures and, if not, develop and implement a training program; and

- ensure that all vulnerabilities identified during vulnerability scanning are remediated in accordance with Federal requirements.

INDIAN HEALTH SERVICE COMMENTS

In written comments, IHS concurred with all of our recommendations and described the actions it had taken and plans to take to implement them. IHS also provided a technical comment regarding vulnerability mitigation timeframes. We addressed the comment and noted IHS's patch management standard operating procedure which requires IHS to approve critical patches to areas/facilities within 5 business days of vendor release and deploy all critical patches within 10 business days of availability to local site servers. IHS's comments, excluding personally identifiable information, are included as Appendix D.

APPENDIX A: FEDERAL REGULATIONS and NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY REQUIREMENTS

FEDERAL REGULATIONS

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (45 CFR § 164.312 (a)(2)(iv)) states that organizations must "implement a mechanism to encrypt and decrypt electronic protected health information."

The HIPAA Security Rule (45 CFR § 164.308(a)(1)) also specifies that entities must "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information ...." HHS's Office for Civil Rights oversees the HIPAA Security Rule and has issued detailed clarifications of required risk assessment elements.

Indian Health Manual

The *Indian Health Manual*, § 8-12.1H(2)(b) states:

> Contingency Planning. Management officials dependent upon IT systems for the support of essential functions are responsible for the development and maintenance of contingency plans for these functions. These contingency plans shall describe the resources and procedures to be used for maintaining the continuity of applications critical to the mission of the IHS in the event of a disaster. These contingency plans shall be reviewed and stored by the ISSO [information system security officer]. Contingency plans for large systems support Area or IHS functions shall be fully documented (JCAHO [Joint Commission on Accreditation of Healthcare Organizations] disaster plan acceptable). Smaller, local systems may have more abbreviated and less formal plans. Each contingency plan shall be tested at least once a year and shall include the following:
>
> (i) Procedures for back-up storage and recovery of data and software, including but not limited to frequency of back-ups, testing of back-ups for usability, and secure off-site storage of back-ups.
>
> (ii) Selection of a back-up or alternate operations strategy.
>
> (iii) Emergency response actions to be taken to protect life and property and to minimize the impact of the emergency.
>
> (iv) Procedures for initiating contingency operations.

(v) Procedures for resumption of normal operations.

(vi) Annual testing procedures.

The *Indian Health Manual*, section 8-12.1H(2)(i), states that security training above the awareness level shall be provided to all personnel who design, implement, or maintain systems.

The *Indian Health Manual*, section 8-19.1D, “Least Privilege,” states:

> It is the policy of the IHS that each IT user will be authorized the most restrictive set of privileges or access needed for performing authorized tasks. All elevated system privilege accounts must be controlled and limited to Office of Information Technology (OIT) support personnel, Area Information Systems Coordinators (ISC), or their designated alternates.

The *Indian Health Manual*, section 3-7.3D (xii)(c)(i), “Controlled Substances c. Storage,” states:

> (i) Pharmacy Stocks
>
> a. Schedule II
>
> Schedule II controlled substances, alcohol, and spirituous liquors shall be stored in a substantially constructed locked cabinet, safe, or drawer.
>
> b. Other Scheduled drugs
>
> Although Federal law allows for the dispersion of Schedule III, IV, and V controlled substances among the regular stock, it is strongly suggested that only a small working stock be dispersed among regular stock with the remainder securely stored under lock and key. Schedule III, IV and V controlled substances stored in Drug-O-Matic cassettes or Baker cells shall be secured under lock and key after pharmacy hours unless access to the pharmacy is solely restricted to pharmacy staff.
>
> A duplicate key or copy of the safe combination shall be kept in a sealed envelope in the service unit director's safe or other secure place for use in emergency situations.

Indian Health Standard Operating Procedure for IHS Enterprise Patch Management

The *Standard Operating Procedure for IHS Enterprise Patch Management*, section 3 Roles and Responsibility for Patch Management, states that enterprise IT shall test all critical patches against standard supported IHS applications and operating systems within three (3) business days after vendor release and ensure availability of approved critical patches to Areas/Facilities within (5) business days of vendor release. Also, area Information System Security Officer shall test all critical security patches against local standard system configurations within three (3) business days of deployment to local site server, and deploy all critical patches to all supported workstations and servers within ten (10) business days of availability to local site server.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY REQUIREMENTS

NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems,* (ES-1), states:

> This guide defines the following seven-step contingency planning process that an organization may apply to develop and maintain a viable contingency planning program for their information systems. These seven progressive steps are designed to be integrated into each stage of the system development life cycle.
>
> 1. Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
> 2. Conduct the business impact analysis (BIA). The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes. A template for developing the BIA is provided to assist the user.
> 3. Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.
> 4. Create contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
> 5. Develop an information system contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.
> 6. Ensure plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.
> 7. Ensure plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

NIST developed SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* to further its statutory responsibilities under the Federal Information Systems Management Act for developing information security standards and guidelines, including minimum requirements for Federal information systems, and is consistent with the requirements of the OMB Circular No. A-130, section 8b(3), "Securing Agency Information Systems."
In its *Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems,* NIST:

> . . . specifies minimum security requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53*, Recommended Security Controls for Federal Information Systems*, as amended*.*

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Appendix F, PE-2 states that the:

> . . . organization . . . issues authorization credentials for facility access . . . enforces physical access authorizations at [*organization-defined entry/exit points to the facility where the information system resides*] by verifying individual access authorizations before granting access to the facility.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Appendix F, AC-1, states that an organization:

> . . . develops, documents, and disseminates . . . [a]n access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and [p]rocedures to facilitate the implementation of the … policy and associated . . . controls (AC-1), (AT-1), (IA-1), (AU-1), (SI-1), (PL-1), (SC-1), and (CM-1).[24]

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations, Appendix F,* SA-22, requires that organizations replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations, Appendix F,* AC-6, requires that the organization employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that

[24] These control numbers refer to security controls and control enhancements listed in NIST SP 800-53, Revision 4, Appendix F.

are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

According to NIST SP 800-30, *Guide for Conducting Risk Assessments,* chapter 2.4.1, comprehensive risk assessments should be conducted on organizational operations, assets, and individuals across mission and business lines.

Also, NIST SP 800-39, *Managing Information Security Risk*, chapter 2.1, *Organization, Mission, and Information System View*, states that:

> . . . the purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations; . . . (iii) the harm (i.e., consequences/ impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring).

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations, Appendix F,* RA-5: *Vulnerability Scanning*, requires organizations to analyze vulnerability scan reports, define personnel or roles with whom information obtained from the vulnerability scanning process should be shared, and share information obtained from the vulnerability scanning process with those personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

APPENDIX B: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed IHS's information system general and physical controls over the dispensing of prescription drugs, including opioids, at two hospitals: Burdick Memorial and Blackfeet Hospital. To accomplish our objective, we used appropriate procedures from applicable Federal regulations and guidance. We reviewed policies and procedures, interviewed staff at IHS headquarters and two IHS hospitals, and reviewed supporting documentation. To identify potential security-related configuration vulnerabilities on IHS's PHR website,[25] we used audit software-scanning programs.

We limited our review to IHS's implementation of certain information and physical system controls supporting the dispensing of prescription drugs. We did not review IHS's overall internal controls. IHS's organizational structure is highly decentralized. Our observations are specific to the two facilitates that we visited, Burdick Memorial and Blackfeet Hospital. We focused on possible drug diversions related to pharmacy operations. We do not opine on the controls across IHS; however, we have included recommendations for IHS to determine if some of the issues we identified are systemic across IHS.

We conducted our fieldwork at Burdick Memorial in Belcourt, North Dakota, from October 31 through November 4, 2016; Blackfeet Hospital in Browning, Montana, from November 14 through 18, 2016; and IHS Headquarters in Rockville, Maryland, from January 23 through 27, 2017.

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal regulations, NIST requirements, and industry best practices;
- interviewed appropriate computer operations personnel responsible for information security at IHS Headquarters and two IHS hospitals;
- at two IHS hospitals and in coordination with IHS Headquarters personnel, analyzed system configuration reports for potential network vulnerabilities, such as patching;
- performed a web application vulnerability scan on the PHR website; and,
- reviewed our findings with IHS management.

[25] Available online at https://phr.ihs.gov; the PHR website is the patient portal for IHS patients.

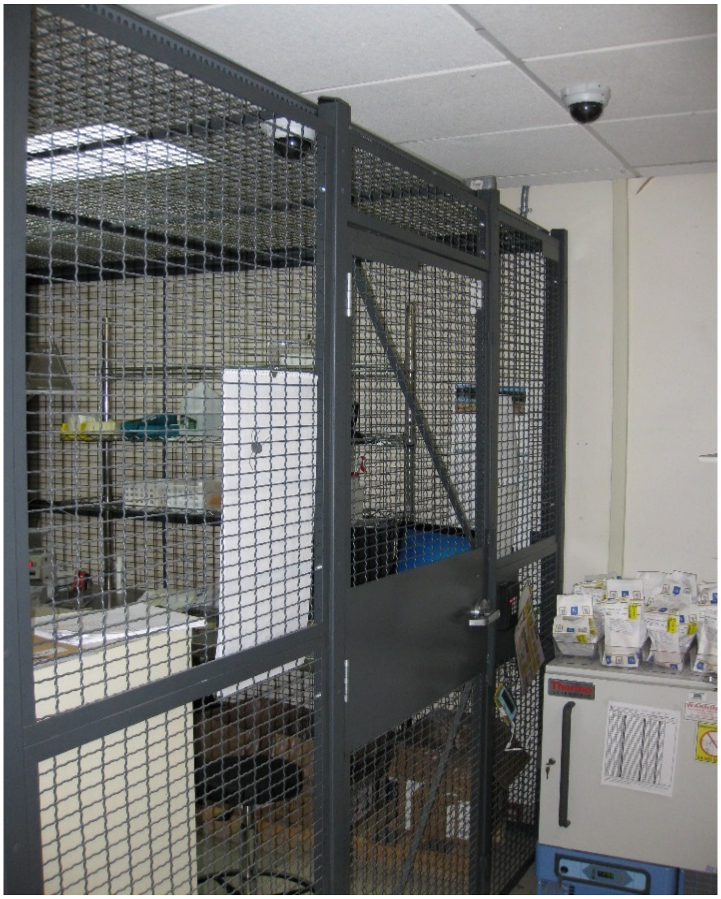
We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We shared with IHS information about our vulnerability scan findings immediately following the scans and informed IHS about other preliminary findings in advance of issuing our draft report.

APPENDIX C: PHOTOGRAPHIC EXAMPLES

Photograph 1: The Pyxis system for tracking prescription drugs at Burdick Memorial.

Photograph 2: Secured compartments of the Pyxis system that keep Scheduled drugs from being dispensed inappropriately at Burdick Memorial.

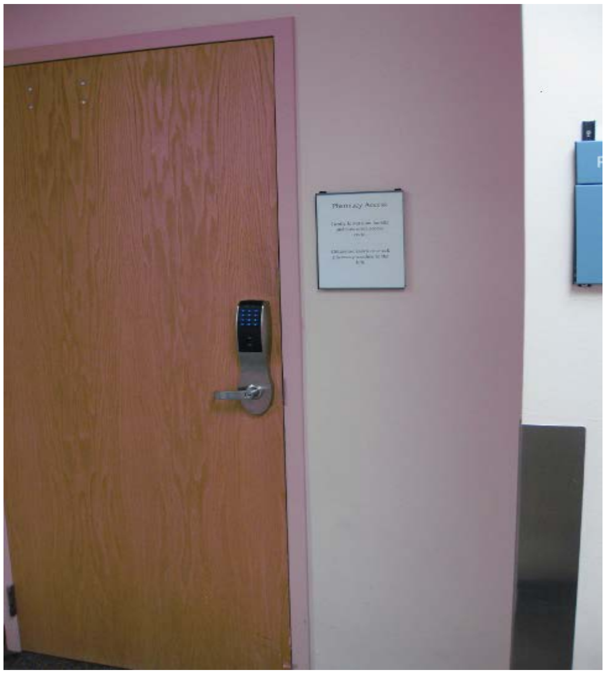
Photo 3: The Pyxis system at Blackfeet Hospital.



Photograph 4: Locked cage inside the pharmacy department where Scheduled drugs were secured at Burdick Memorial.

Photograph 5: Prescription pickup window monitored by a surveillance camera at Burdick Memorial.

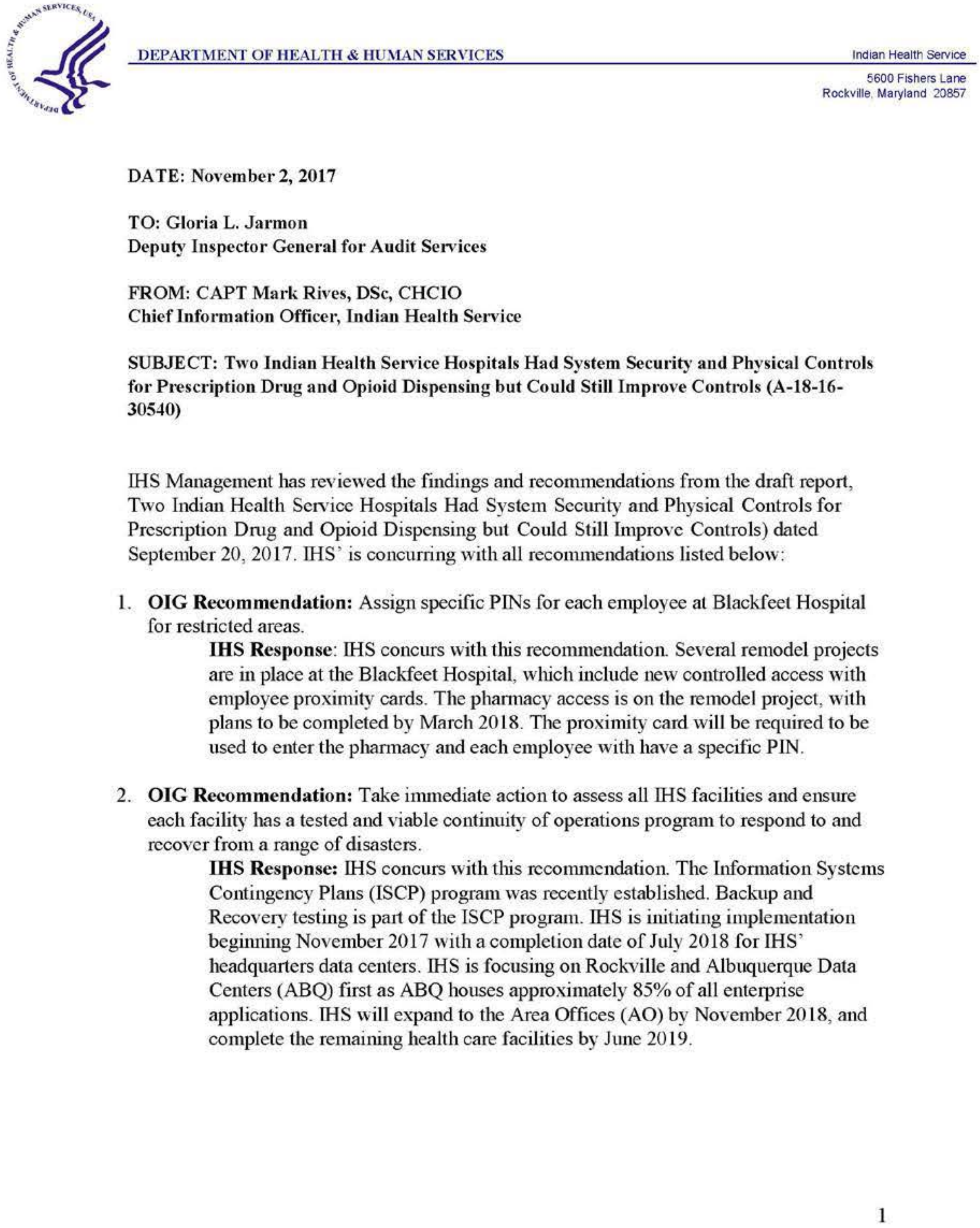
Photograph 6: Entrance to the secured pharmacy area protected by badge and PIN code access at Burdick Memorial.



Photograph 7: Entrance to the secured pharmacy area protected by PIN code access at Blackfeet Hospital.

Photograph 8: The server rack at Burdick Memorial.

APPENDIX D: INDIAN HEALTH SERVICE COMMENTS



DEPARTMENT OF HEALTH & HUMAN SERVICES

Indian Health Service
5600 Fishers Lane
Rockville, Maryland 20857

DATE: November 2, 2017

TO: Gloria L. Jarmon
Deputy Inspector General for Audit Services

FROM: CAPT Mark Rives, DSc, CHCIO
Chief Information Officer, Indian Health Service

SUBJECT: Two Indian Health Service Hospitals Had System Security and Physical Controls for Prescription Drug and Opioid Dispensing but Could Still Improve Controls (A-18-16-30540)

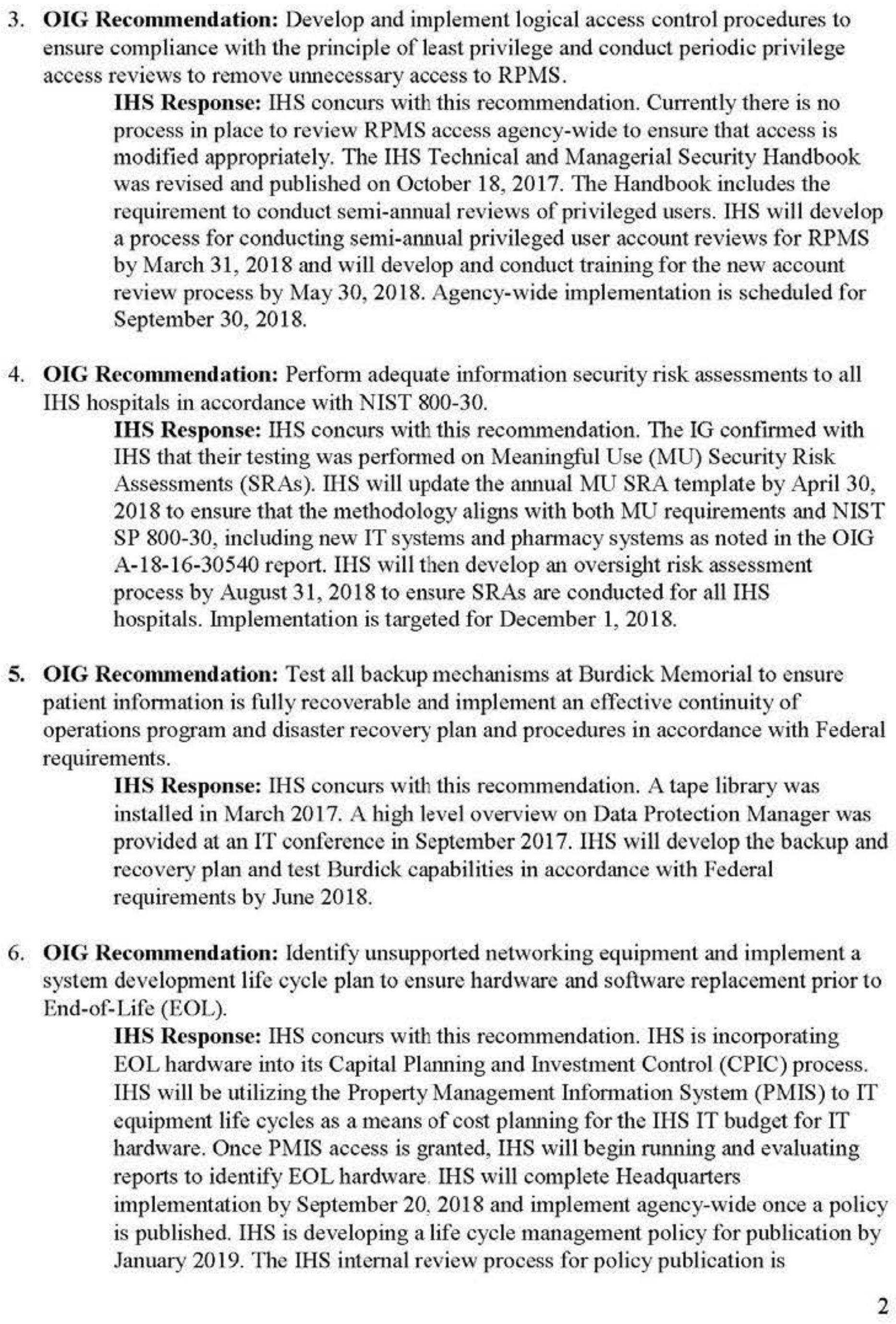
IHS Management has reviewed the findings and recommendations from the draft report, Two Indian Health Service Hospitals Had System Security and Physical Controls for Prescription Drug and Opioid Dispensing but Could Still Improve Controls) dated September 20, 2017. IHS' is concurring with all recommendations listed below:

1. **OIG Recommendation:** Assign specific PINs for each employee at Blackfeet Hospital for restricted areas.

   IHS Response: IHS concurs with this recommendation. Several remodel projects are in place at the Blackfeet Hospital, which include new controlled access with employee proximity cards. The pharmacy access is on the remodel project, with plans to be completed by March 2018. The proximity card will be required to be used to enter the pharmacy and each employee with have a specific PIN.

2. **OIG Recommendation:** Take immediate action to assess all IHS facilities and ensure each facility has a tested and viable continuity of operations program to respond to and recover from a range of disasters.

   IHS Response: IHS concurs with this recommendation. The Information Systems Contingency Plans (ISCP) program was recently established. Backup and Recovery testing is part of the ISCP program. IHS is initiating implementation beginning November 2017 with a completion date of July 2018 for IHS' headquarters data centers. IHS is focusing on Rockville and Albuquerque Data Centers (ABQ) first as ABQ houses approximately 85% of all enterprise applications. IHS will expand to the Area Offices (AO) by November 2018, and complete the remaining health care facilities by June 2019.



3. **OIG Recommendation:** Develop and implement logical access control procedures to ensure compliance with the principle of least privilege and conduct periodic privilege access reviews to remove unnecessary access to RPMS.

   IHS Response: IHS concurs with this recommendation. Currently there is no process in place to review RPMS access agency-wide to ensure that access is modified appropriately. The IHS Technical and Managerial Security Handbook was revised and published on October 18, 2017. The Handbook includes the requirement to conduct semi-annual reviews of privileged users. IHS will develop a process for conducting semi-annual privileged user account reviews for RPMS by March 31, 2018 and will develop and conduct training for the new account review process by May 30, 2018. Agency-wide implementation is scheduled for September 30, 2018.

4. **OIG Recommendation:** Perform adequate information security risk assessments to all IHS hospitals in accordance with NIST 800-30.

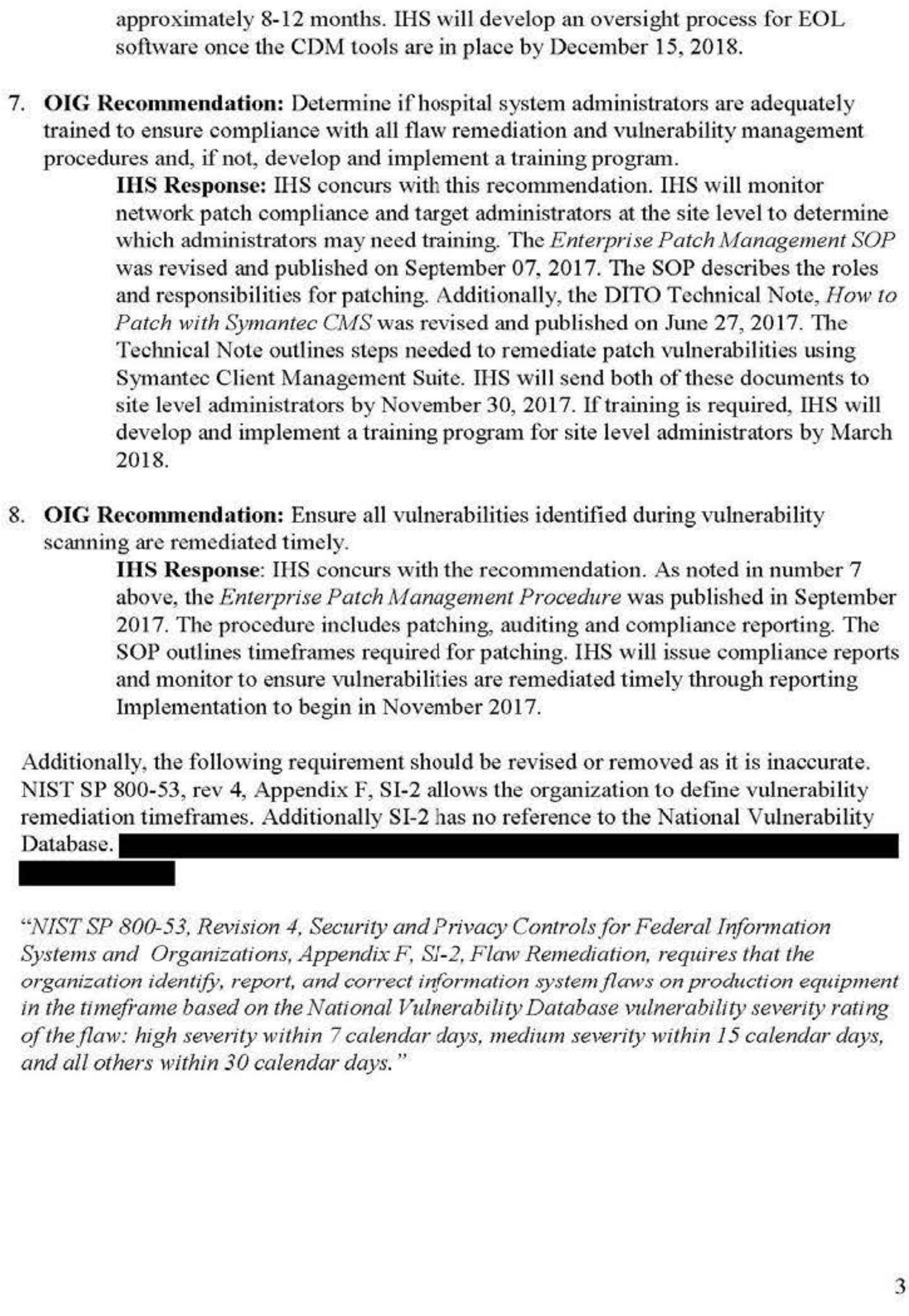
   IHS Response: IHS concurs with this recommendation. The IG confirmed with IHS that their testing was performed on Meaningful Use (MU) Security Risk Assessments (SRAs). IHS will update the annual MU SRA template by April 30, 2018 to ensure that the methodology aligns with both MU requirements and NIST SP 800-30, including new IT systems and pharmacy systems as noted in the OIG A-18-16-30540 report. IHS will then develop an oversight risk assessment process by August 31, 2018 to ensure SRAs are conducted for all IHS hospitals. Implementation is targeted for December 1, 2018.

5. **OIG Recommendation:** Test all backup mechanisms at Burdick Memorial to ensure patient information is fully recoverable and implement an effective continuity of operations program and disaster recovery plan and procedures in accordance with Federal requirements.

   IHS Response: IHS concurs with this recommendation. A tape library was installed in March 2017. A high level overview on Data Protection Manager was provided at an IT conference in September 2017. IHS will develop the backup and recovery plan and test Burdick capabilities in accordance with Federal requirements by June 2018.

6. **OIG Recommendation:** Identify unsupported networking equipment and implement a system development life cycle plan to ensure hardware and software replacement prior to End-of-Life (EOL).

   IHS Response: IHS concurs with this recommendation. IHS is incorporating EOL hardware into its Capital Planning and Investment Control (CPIC) process. IHS will be utilizing the Property Management Information System (PMIS) to IT equipment life cycles as a means of cost planning for the IHS IT budget for IT hardware. Once PMIS access is granted, IHS will begin running and evaluating reports to identify EOL hardware. IHS will complete Headquarters implementation by September 20, 2018 and implement agency-wide once a policy is published. IHS is developing a life cycle management policy for publication by January 2019. The IHS internal review process for policy publication is



approximately 8-12 months. IHS will develop an oversight process for EOL software once the CDM tools are in place by December 15, 2018.

7. **OIG Recommendation:** Determine if hospital system administrators are adequately trained to ensure compliance with all flaw remediation and vulnerability management procedures and, if not, develop and implement a training program.

    IHS Response: IHS concurs with this recommendation. IHS will monitor network patch compliance and target administrators at the site level to determine which administrators may need training. The *Enterprise Patch Management SOP* was revised and published on September 07, 2017. The SOP describes the roles and responsibilities for patching. Additionally, the DITO Technical Note, *How to Patch with Symantec CMS* was revised and published on June 27, 2017. The Technical Note outlines steps needed to remediate patch vulnerabilities using Symantec Client Management Suite. IHS will send both of these documents to site level administrators by November 30, 2017. If training is required, IHS will develop and implement a training program for site level administrators by March 2018.

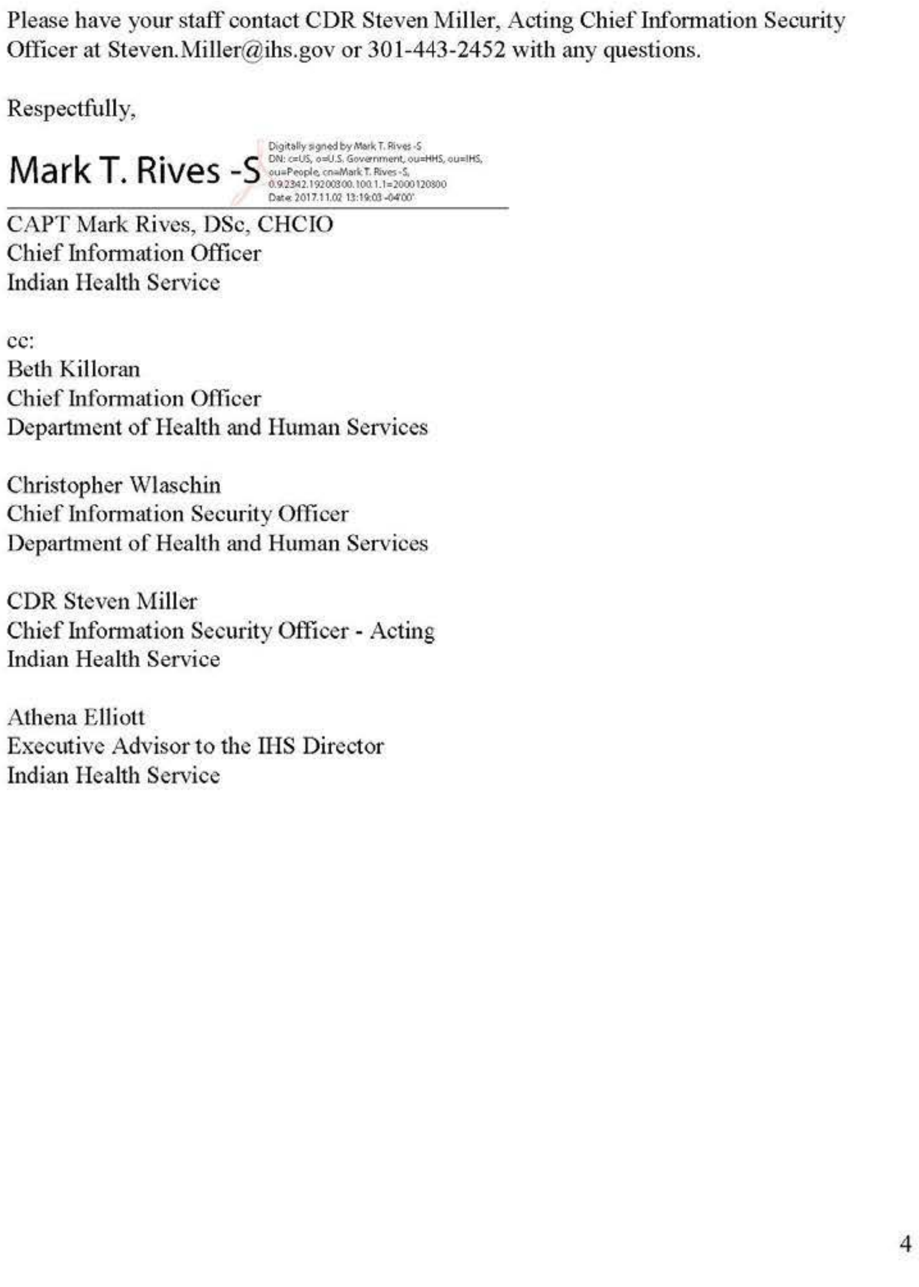
8. **OIG Recommendation:** Ensure all vulnerabilities identified during vulnerability scanning are remediated timely.

    IHS Response: IHS concurs with the recommendation. As noted in number 7 above, the *Enterprise Patch Management Procedure* was published in September 2017. The procedure includes patching, auditing and compliance reporting. The SOP outlines timeframes required for patching. IHS will issue compliance reports and monitor to ensure vulnerabilities are remediated timely through reporting Implementation to begin in November 2017.

Additionally, the following requirement should be revised or removed as it is inaccurate. NIST SP 800-53, rev 4, Appendix F, SI-2 allows the organization to define vulnerability remediation timeframes. Additionally SI-2 has no reference to the National Vulnerability Database. [redacted]

"NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Appendix F, SI-2, Flaw Remediation, requires that the organization identify, report, and correct information system flaws on production equipment in the timeframe based on the National Vulnerability Database vulnerability severity rating of the flaw: high severity within 7 calendar days, medium severity within 15 calendar days, and all others within 30 calendar days."

OIG Note - The above text has been redacted because it contains personally identifiable information.



Please have your staff contact CDR Steven Miller, Acting Chief Information Security Officer at Steven.Miller@ihs.gov or 301-443-2452 with any questions.

Respectfully,

Mark T. Rives -S

Digitally signed by Mark T. Rives -S
DN: c=US, o=U.S. Government, ou=HHS, ou=IHS,
ou=People, cn=Mark T. Rives -S,
0.9.2342.19200300.100.1.1=2000120800
Date: 2017.11.02 13:19:03 -04'00'

CAPT Mark Rives, DSc, CHCIO
Chief Information Officer
Indian Health Service

cc:
Beth Killoran
Chief Information Officer
Department of Health and Human Services

Christopher Wlaschin
Chief Information Security Officer
Department of Health and Human Services

CDR Steven Miller
Chief Information Security Officer - Acting
Indian Health Service

Athena Elliott
Executive Advisor to the IHS Director
Indian Health Service