Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

IHS NEEDS TO IMPROVE OVERSIGHT OF ITS HOSPITALS' OPIOID PRESCRIBING AND DISPENSING PRACTICES AND CONSIDER CENTRALIZING ITS INFORMATION TECHNOLOGY FUNCTIONS

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

Joanne M. Cheidi
Acting Inspector General

July 2019
A-18-17-11400

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 Web site.

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: July 2019
Report No. A-18-17-11400

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

IHS Needs To Improve Oversight of Its Hospitals' Opioid Prescribing and Dispensing Practices and Consider Centralizing Its Information Technology Functions

Why OIG Did This Review

Prescription opioids continue to contribute to the opioid overdose epidemic. A prior OIG audit identified high volumes of opioid purchases in IHS communities. In addition, the prior OIG audit of two IHS hospitals determined that IHS did not have adequate information technology (IT) security controls to protect health information and patient safety. The audit also found significant differences in the way the two hospitals carried out their respective IT operations.

We conducted this audit to analyze and compare opioid prescribing and dispensing practices and IT operations at five other IHS hospitals.

Our objectives were to determine whether (1) the hospitals we reviewed prescribed and dispensed opioids in accordance with IHS policies and procedures and (2) IHS's decentralized IT management structure affected its ability to deliver adequate IT and information security services at its hospitals in accordance with Federal requirements.

How OIG Did This Review

We reviewed IHS's opioid prescribing and dispensing practices and information system general controls at five IHS hospitals. In addition, we reviewed a judgmental sample of 150 patients' records. Also, we performed a penetration test at each hospital.

What OIG Found

The IHS hospitals we reviewed did not always follow the Indian Health Manual when prescribing and dispensing opioids. Specifically, through our patient record review, we found that hospitals did not always review the course of patient treatment and causes of pain within required timeframes, perform the required urine drug screenings within recommended time intervals, review patient health records before filling a prescription from a non-IHS provider, and maintain pain management documents to support that provider responsibilities had been performed. We also found that these IHS hospitals did not fully use the States' prescription drug monitoring programs when prescribing or dispensing opioids.

IHS's decentralized IT management structure led to vulnerabilities and weaknesses in implementing security controls at all five hospitals. IHS's controls were not effective at preventing or detecting our penetration test cyberattacks. In addition, the hospitals implemented IT security controls to protect health information and patient safety differently. Inconsistencies in the delivery of cybersecurity services can lead to the same vulnerability being remediated at one hospital but being exploited at another hospital that did not remediate the vulnerability. As a result, IHS hospital operations and delivery of patient care could have been significantly affected.

What OIG Recommends and IHS Comments

We recommend that IHS work with hospitals to ensure they follow the Indian Health Manual when prescribing and dispensing opioids. We also recommend that IHS consider centralizing its IT systems, services, and functions by conducting a cost-benefit analysis of adopting a cloud computing policy, including centralization of IT systems, services, and functions. We made other procedural recommendations, which are listed in the report. We provided more detailed information and specific recommendations to IHS so that it can address specific vulnerabilities that we identified.

In written comments to our draft report, IHS concurred with our recommendations and described actions it has taken or plans to take to address our findings.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

Prescription opioids continue to contribute to the opioid overdose epidemic. An Office of Inspector General (OIG) investigation identified challenges in the Indian Health Service's (IHS's) physical and internal controls over the security of prescription drugs such as opioids.[1] We also identified high volumes of opioid purchases in IHS communities during a prior audit of two IHS hospitals but did not perform a detailed analysis of IHS opioid prescribing practices. In that audit, we determined that IHS did not have adequate IT security controls to protect health information and patient safety.[2] That audit also found significant differences in the way the two hospitals carried out their respective IT operations. This audit analyzed and compared opioid prescribing and dispensing[3] practices and IT operations at five IHS hospitals.[4]

OBJECTIVES

Our objectives were to determine (1) whether the hospitals we reviewed prescribed and dispensed opioids in accordance with IHS policies and procedures and (2) whether IHS's decentralized IT management structure had affected its ability to deliver adequate IT and information security services at its hospitals in accordance with Federal requirements.

BACKGROUND

Indian Health Service

IHS provides comprehensive healthcare services to approximately 2.6 million American Indians and Alaska Natives (AI/ANs) and has an annual budget of $5.6 billion. IHS's mission is "to raise the physical, mental, social, and spiritual health of American Indians and Alaska Natives to the highest level."[5] IHS facilities include 24 hospitals, 50 health centers, and 24 health stations. In providing healthcare services, including prescribing and dispensing opioids, IHS is responsible

[1] Opioids, such as hydrocodone, oxycodone, morphine, and methadone, are prescribed to treat both acute and chronic pain. Because many opioids have a high potential for abuse and may lead to severe psychological or physical dependence, many of them are classified as Schedule II drugs under the Controlled Substances Act.

[2] *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, November 2017). Available online at https://oig.hhs.gov/oas/reports/region18/181630540.pdf.

[3] In this report, "prescribing" is a provider writing a prescription for a patient, while "dispensing" is a pharmacist filling the prescription.

[4] This audit analyzed these two areas separately and the findings and recommendations for each area are not related. We reported on these two areas together because we conducted them at the same time at the same IHS facilities.

[5] https://www.ihs.gov/aboutihs/. Accessed on June 11, 2018.

for securing the information that it collects, records, transmits, and uses in the performance of its mission.

IHS has a decentralized management structure that is separated into two major components: headquarters offices and 12 area offices. Area offices are in multiple, and sometimes remote, locations and support Federal and tribal hospitals in specific regions of the United States.[6] IHS headquarters issues guidance for area offices and IHS hospitals. In addition, IHS headquarters maintains the Indian Health Manual (IHM), which defines headquarters' and area offices' responsibilities, including their responsibilities for prescribing and dispensing opioids.

IHS Efforts To Combat Opioid Epidemic

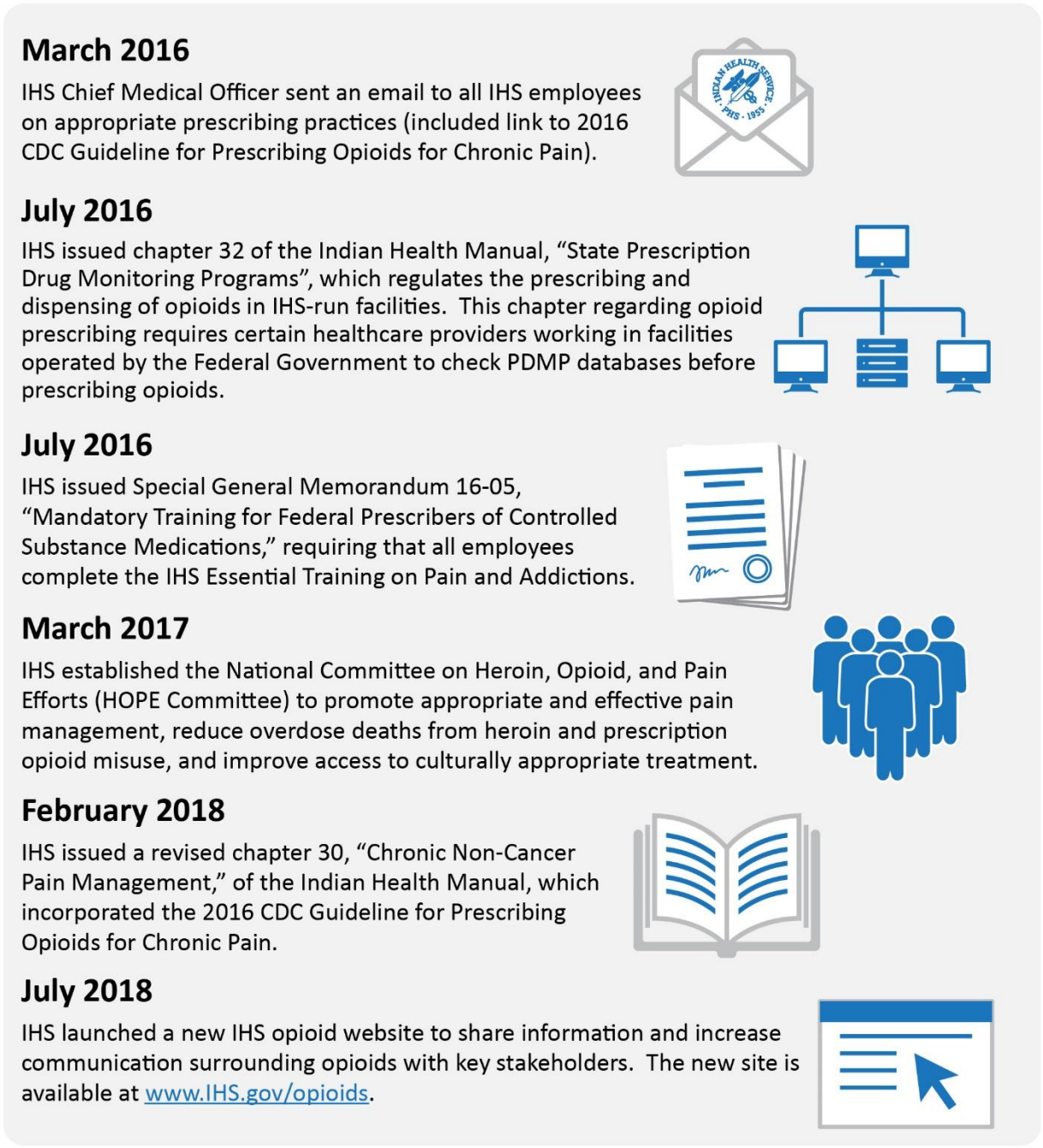
More than 40 percent of all U.S. opioid overdose deaths in 2016 involved a prescription opioid, and more than 46 people die every day from overdoses involving prescription opioids.[7] The Centers for Disease Control and Prevention (CDC) reported that AI/AN communities had the highest drug overdose death rates in 2015 and the largest percentage increase in deaths from 1999 to 2015 when compared with other racial and ethnic groups.[8] IHS has recognized the opioid epidemic facing the AI/AN communities, and over the past 2 years, it has battled the epidemic in numerous ways. Figure 1 on the following page highlights these efforts.

[6] The area offices are located in Aberdeen, South Dakota; Albuquerque, New Mexico; Anchorage, Alaska; Bemidji, Minnesota; Billings, Montana; Nashville, Tennessee; Oklahoma City, Oklahoma; Portland, Oregon; Phoenix, Arizona; Sacramento, California; Tucson, Arizona; and Window Rock/Navajo, Arizona.

[7] https://www.cdc.gov/drugoverdose/data/overdose.html. Accessed on August 15, 2018.

[8] Center for Disease Control and Prevention, "Illicit Drug Use, Illicit Drug Use Disorders, and Drug Overdose Deaths in Metropolitan and Nonmetropolitan Areas – United States", *Morbidity and Mortality Weekly Report*, October 20, 2017; page 5. Available at https://www.cdc.gov/mmwr/volumes/66/ss/pdfs/ss6619.pdf. Accessed on December 3, 2018.

Figure 1: IHS Efforts To Combat the Opioid Epidemic



Prescription Drug Monitoring Program

The IHM states that State prescription drug monitoring programs (PDMPs) are tools for providers and pharmacists to monitor and deter prescription medication misuse, abuse, addiction, and diversion and to help ensure appropriate clinical care. The PDMPs are State-based, electronic databases that collect data on controlled medications dispensed by registered pharmacies operating within the State (IHM 3-32.1B). Implementing chapter 32 of the IHM will

help IHS improve appropriate pain management care, identification of patients struggling with opioid abuse, and diversion[9] prevention.

Use of Opioids for Pain Management

IHS is committed to ensuring appropriate management of chronic non-cancer pain to improve patients' daily function and quality of life through prompt and effective assessment, diagnosis, and treatment.[10] This type of care, however, comes with certain risks. The IHS's policies regarding managing chronic non-cancer pain mitigates some of these risks and ensures use of opioids for legitimate medical purposes and in the course of professional practice. IHS considers prescribing and dispensing of opioids for pain to be for a legitimate medical purpose if it is based on a provider's[11] knowledge of effective treatment modalities and sound clinical judgment. For opioids to be administered within the usual course of professional practice, a provider–patient relationship must exist.[12] Figure 2 depicts the IHM's process for prescribing opioids to treat chronic non-cancer pain management.

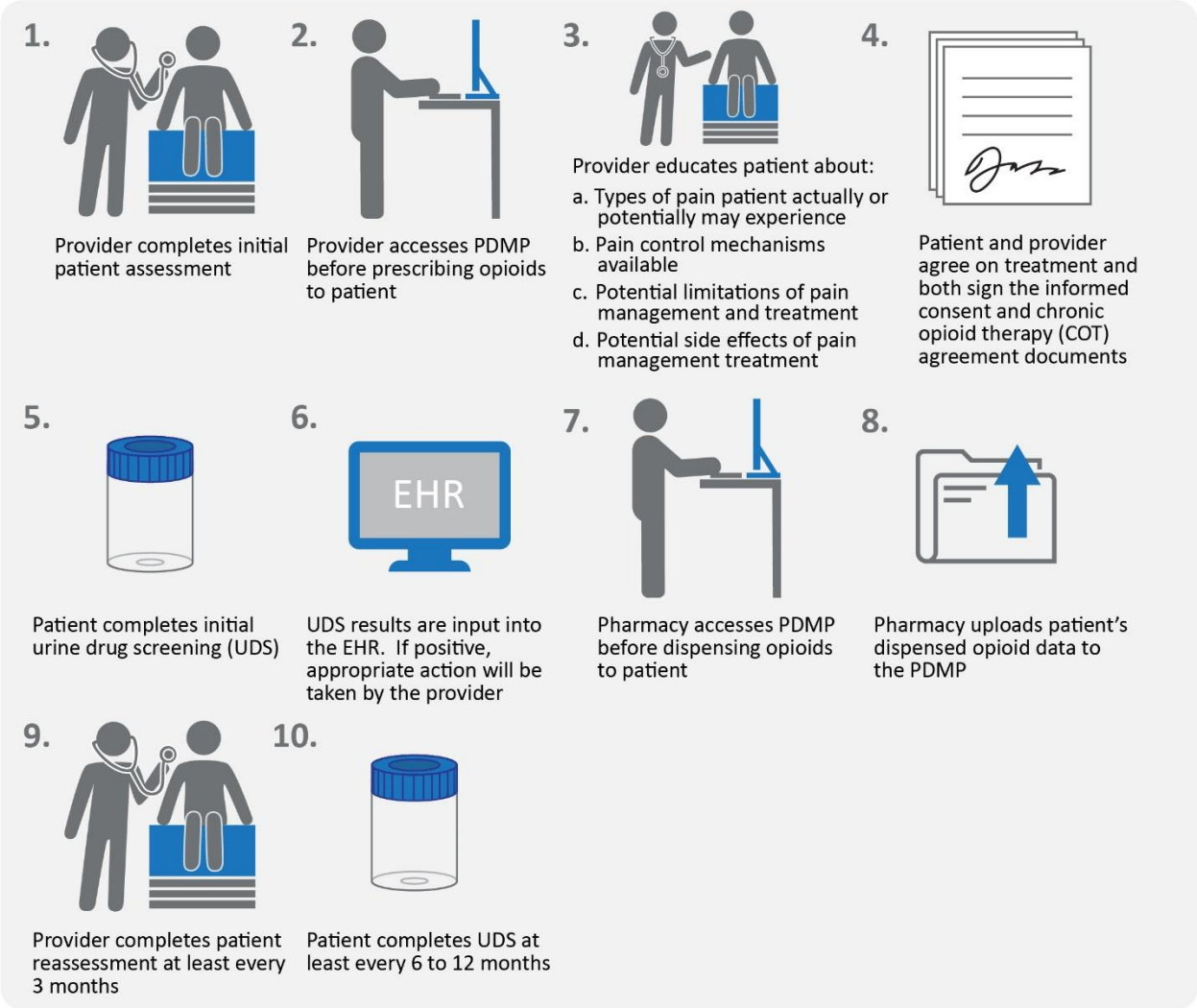
[9] Diversion of controlled substances refers to legally obtainable drugs that are diverted from the individual prescribed the medication to another person or into illegal channels or when controlled substances are obtained by an illegal method (IHM 3-30.1F(8)).

[10] IHM 3-30.1(E). During February 2018, IHS updated IHM, part 3, chapter 30, "Chronic Non-Cancer Pain Management." We used the June 2014 edition of the IHM because it was effective during our audit period.

[11] For purposes of this report, "provider" and "prescriber" are interchangeable.

[12] IHM 3-30.3(F).

Figure 2: Process of Care for Chronic Non-Cancer Pain Management in IHS



Resource and Patient Management System

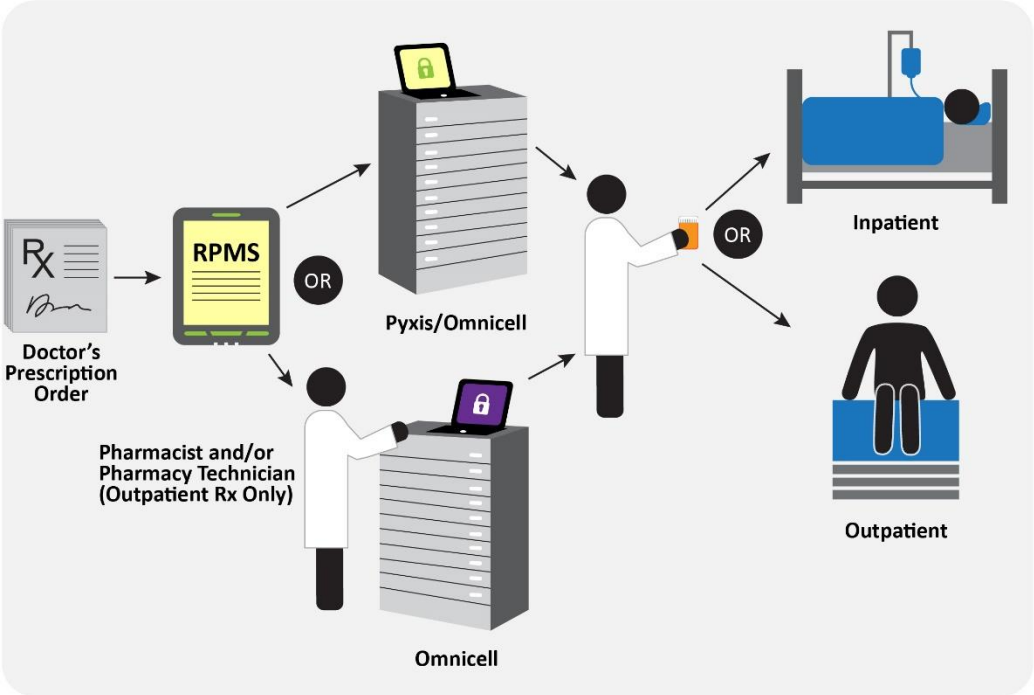
One of IHS's major investments in health IT is its Resource and Patient Management System (RPMS). It is designed to operate on computers located at more than 400 IHS, tribal, and urban Indian health facilities. The IHS Office of Information Technology is primarily responsible for the development and distribution of the 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. In addition, the RPMS is an automated information system consisting of more than 60 integrated software applications.

Electronic health record (EHR) system is one of the integrated software applications of the RPMS. EHR helps providers manage all aspects of patient care electronically, by providing a full range of functions for data retrieval and capture to support patient review, encounter, and follow-up.

Medication Dispensing Systems

The hospitals we visited used medication dispensing systems. These systems support medication management with various features for safety and efficiency. Also, the systems help accurately dispense medication, while supporting pharmacy workflows. The hospitals we reviewed had two types of medication dispensing systems, Pyxis and Omnicell, both of which work in conjunction with the RPMS. Pyxis receives inpatient and outpatient prescription data via a one-way communication link from RPMS. Omnicell receives inpatient prescription data via a one-way communication link from RPMS. For outpatient prescriptions data, a pharmacist or other pharmacy employee must enter the data manually in the Omnicell. Three hospitals used Pyxis, and two hospitals used Omnicell. Figure 3 depicts their prescription drug dispensing process.

Figure 3: Prescription Drug Dispensing Process in Five IHS Hospitals



IHS's Information Technology Management Structure

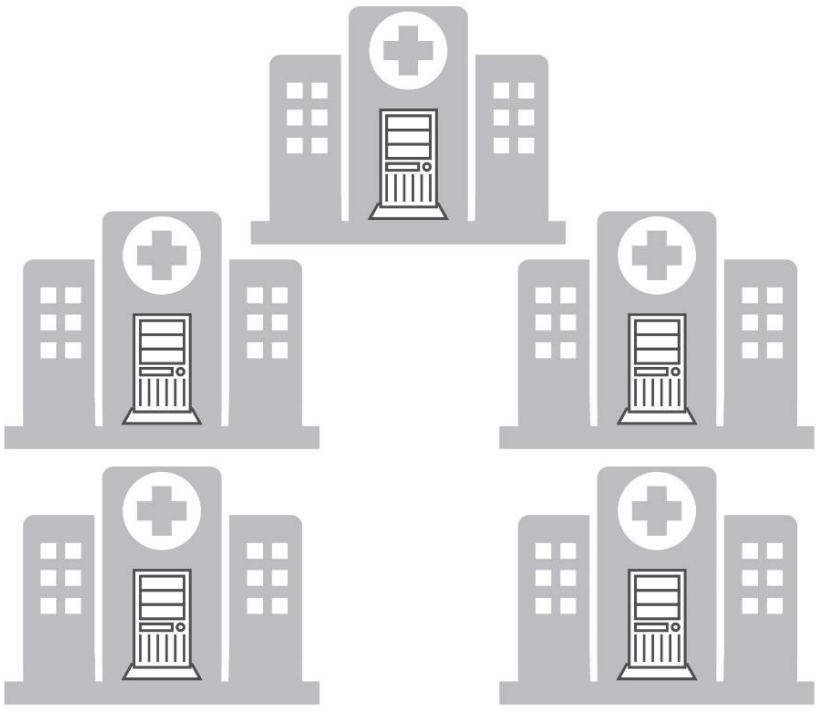
IHS currently has a decentralized IT management structure. Currently IHS essentially operates separate mini-networks at each of its 25 hospitals. Each IHS hospital, service unit, and area office manages some or all of its own servers, switches, routers, internet connection, physical controls, patch management, cabling, and user support. IHS hospitals receive varying levels of support from their area offices. IHS headquarters personnel issue policy, provide guidance, scan the IHS network, and provide IT funding to area offices and hospitals. See Figure 4 on the following page.

Centralization of Information Technology

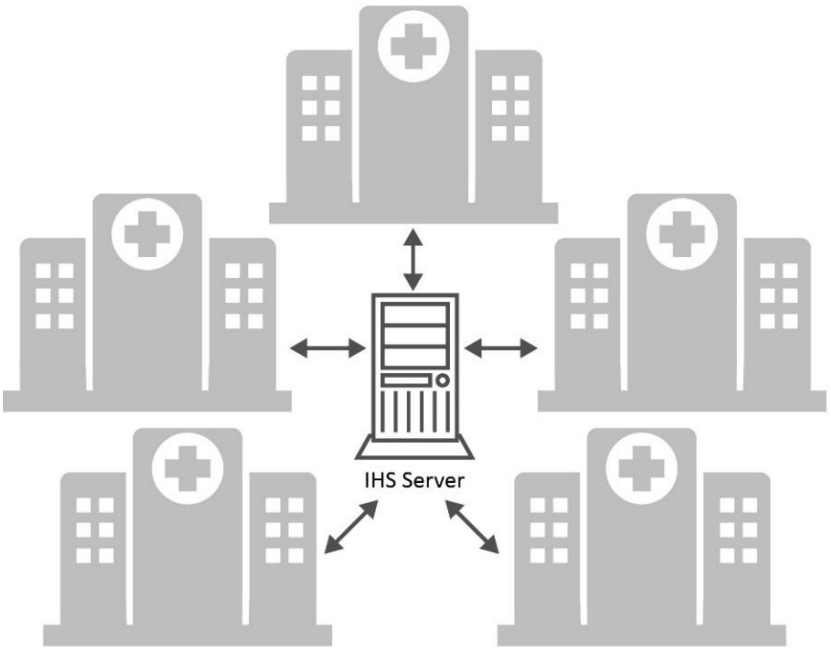
Centralization of IT could include having servers at a central location (e.g., area office, IHS headquarters) or in the cloud or a combination of both. Benefits of centralizing servers and hardware assets include the potential for cost savings, reduced responsibilities for IT hospital staff so they can focus on user support, and oversight of fewer locations for senior IT management. The centralization of IT assets would also likely be accompanied by changes in the IT management structure, and strategic determinations would be required by senior IT personnel.

Figure 4: Decentralization vs. Centralization of Hospital IT Services

Decentralized Set-Up



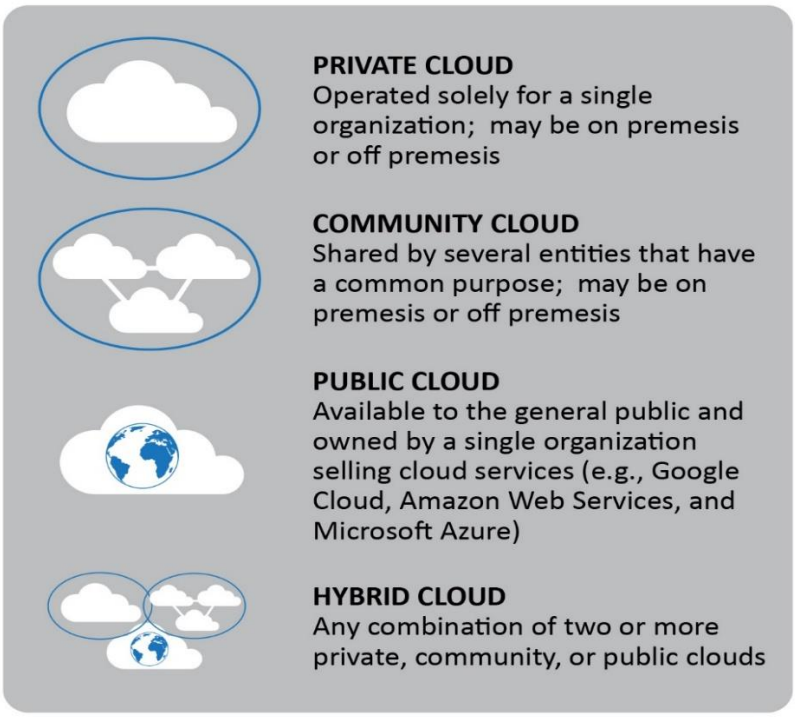
Centralized Set-Up



Cloud Computing

Cloud computing offers several deployment models, each of which provides distinct trade-offs: Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud (Figure 5).

Figure 5: Types of Cloud Models



Cloud First Policy

In 2011, the White House issued the *Federal Cloud Computing Strategy*, which states on page 2:

> To harness the benefits of cloud computing, we have instituted a Cloud First policy. This policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.
>
> By leveraging shared infrastructure and economies of scale, cloud computing presents a compelling business model for Federal leadership. Organizations will be able to measure and pay for only the IT resources they consume, increase or decrease their usage to match requirements and budget constraints, and leverage the shared underlying capacity of IT resources via a network. Resources needed to support mission critical capabilities can be provisioned more rapidly and with minimal overhead and routine provider interaction.

Cloud Computing Challenges

Adopting an effective cloud computing strategy presents challenges for any organization, particularly one that has a history of operating disparate networks. The Federal Cloud & Data Center Summit [13], held in June 2018, included representatives from industry, academia and government. Barriers and challenges were identified when adopting a cloud solution, which included: long acquisition cycles; lack of strategic direction and approaches; difficulty performing organizational transformation (people, process and technology to support digital transformation) and driving change through building next-generation cloud-native apps. Some of the challenges identified may not be the exact problems that IHS will confront. However, significant IT transformation and modernization will present challenges that require strategic planning and management.

HOW WE CONDUCTED THIS REVIEW

We reviewed IHS's opioid prescribing and dispensing practices and information system general controls at five IHS hospitals: Cass Lake Hospital in Cass Lake, Minnesota (Cass Lake); Fort Yates Hospital in Fort Yates, North Dakota (Fort Yates); Lawton Indian Hospital in Lawton, Oklahoma (Lawton); Phoenix Indian Medical Center in Phoenix, Arizona (Phoenix); and Northern Navajo Medical Center in Shiprock, New Mexico (Northern Navajo).

For the opioid prescribing and dispensing objective of the audit, we reviewed IHS and hospital policies and procedures and interviewed IHS hospital staff. We tested patients' records for

[13] https://www.mitre.org/sites/default/files/publications/PRS18-2725-1_june2018_federal_cloud__data_center_summit_report.pdf. Accessed on February 27, 2019.

compliance with IHS policies and procedures using a checklist we developed based on the IHM. We judgmentally selected a sample of 30 patient records from each of the five hospitals for a total of 150 patient records. We selected patient records in four categories: (1) patients who were dispensed opioids with daily morphine milligram equivalents (MMEs)[14] of above 30, (2) patients who were dispensed opioids with daily MMEs of 30 and below, (3) patients who received opioids for more than 90 days, and (4) patients with prescriptions for opioids written by non-IHS providers. We did not include patients taking opioids for treatment of cancer related pain.

To determine the impact of IHS's decentralized IT management structure on the delivery of IT and information security services, we reviewed IHS policies and procedures, interviewed hospital staff, and reviewed supporting documentation. We also conducted penetration testing[15] at each hospital. We contracted with Defense Point Security (DPS) to conduct the penetration testing on our behalf.

We limited our review to IHS's implementation of certain internal controls and IT controls. Our observations were specific to the five IHS-operated facilities that we visited, although some of our observations could apply more broadly because they were systemic in all five hospitals. Therefore, we have recommendations for IHS to implement additional controls, including policies and procedures that will affect all IHS Federal facilities. We shared with IHS information about our preliminary findings before issuing our draft report. We also provided more detailed information and specific recommendations to IHS so that it can address specific vulnerabilities that we identified.

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.

Appendix A contains the details of our audit scope and methodology.

FINDINGS

We found that the five IHS hospitals did not always prescribe and dispense opioids in accordance with IHS policies and procedures. We also found that IHS did not have adequate cybersecurity and IT services at its hospitals in accordance with Federal requirements.

[14] MME, also referred to as morphine equivalent dose, refers to a numerical standard to approximate an opioid's potency when compared with a morphine dose standard.

[15] Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. It often involves launching real attacks on real systems and data using tools and techniques commonly used by attackers.

The IHS hospitals we reviewed did not always follow the IHM when prescribing and dispensing opioids. Specifically, through our patient record review, we found that hospitals did not always (1) review the course of patient treatment and causes of pain within required timeframes; (2) perform the required urine drug screenings (UDSs) within recommended time intervals; (3) review patient health records before filling a prescription from a non-IHS provider; and (4) maintain pain management documents to support that the provider had performed his or her responsibilities. We also found that IHS hospitals did not fully use the States' PDMPs when prescribing or dispensing opioids. Specifically, hospitals (1) did not always update their State's PDMP with opioid dispensing data within required timeframes, (2) did not provide support that providers always checked the PDMP before prescribing or dispensing opioids, and (3) could not ensure that providers' PDMP monthly self-audits were performed and a copy sent to the hospital clinical director. IHS hospitals did not always ensure opioids were physically secure before the prescribing or dispensing of opioids. Also, through our analysis of hospital dispensing data, we found that hospitals did not always use available data to identify risks in their prescribing and dispensing practices, such as giving patients (1) opioid doses of as high as 500 daily MMEs and (2) opioids and benzodiazepines at the same time.[16] Additionally, we found that area offices did not always perform required IHS hospital reviews. Hospitals' failure to always prescribe and dispense opioids in accordance with IHS policies and procedures increased the risk of opioid abuse, misuse, and overdose.

IHS's decentralized IT management structure led to vulnerabilities and weaknesses in implementing security controls at all five hospitals. IHS's controls were not effective at preventing or detecting our penetration test cyberattacks. The likely level of sophistication needed to exploit and compromise IHS systems was low, as the attacks did not require significant technical knowledge or extended attacks to exploit IHS systems. In addition, the hospitals implemented IT security controls to protect health information and patient safety differently. Inconsistencies in the delivery of cybersecurity services could have led to the same vulnerability being remediated at one hospital but being exploited at another hospital that did not remediate the vulnerability. As a result, IHS hospital operations and delivery of patient care could have been significantly affected.

IHS HOSPITALS DID NOT ALWAYS FOLLOW POLICIES AND PROCEDURES FOR PRESCRIBING AND DISPENSING OPIOIDS

On the basis of our interviews with hospital personnel, hospital walkthroughs, and sample review of patient records, we found that hospitals did not always ensure that their staff (1) evaluate patient treatment in accordance with IHS policy (five hospitals), (2) perform UDSs within recommended time intervals (five hospitals), (3) review patient health records before filling a prescription from a non-IHS provider (four hospitals), and (4) maintain pain

[16] CDC states that concurrent use of opioids and benzodiazepines puts patients at greater risk of a potentially fatal overdose (CDC, *Guideline for Prescribing Opioids for Chronic Pain – United States*, 2016; available online at https://www.cdc.gov/mmwr/volumes/65/rr/rr6501e1.htm and accessed on March 5, 2018).

management documents to support that provider had performed their responsibilities (five hospitals).

See Appendix C for details of findings related to our review of patient records by hospital.

Patient Treatment Was Not Always Evaluated in Accordance With IHS Policy

The IHM states that at reasonable intervals based on the individual circumstances of the patient in pain but at least every 3 months, the provider should review the patient's course of treatment and any new information about the cause of the pain. Whether the provider continues or modifies therapy depends on the provider's evaluation of the patient's progress toward the stated treatment objectives and goals. Examples of areas that may be evaluated include improvement in the patient's pain intensity and improved physical and psychosocial function (e.g., the ability to work, need for healthcare resources, participation in activities of daily living, and quality of social life) (IHM 3.30.9.C).

At the five hospitals, we found that 30 of the 118 patient records[17] did not include evidence that providers had evaluated patients' treatment at least every 3 months.[18] In addition, during our site visit at Cass Lake, we noticed that the required training,[19] "IHS Essential Training on Pain and Addictions," conflicted with the IHM. (Also, see Figure 1: Timeline of Events in the Background section of this report.) The training materials stated that the patient's treatment was to be reviewed every 6 months instead of every 3 months. After our site visit, we notified IHS headquarters about the conflict, and IHS has since corrected the training materials to match the IHM 3-month requirement.

Hospital officials told us that patients were not always able to come in to the hospital for evaluation because of scheduling and logistic issues, such as the patient's distance from the hospital. Also, some providers told us it was hard to manage treatment, especially when they had to evaluate a high number of patients. When providers do not review the course of treatment at least every 3 months, patient quality of care is compromised, and there may be instances of over- or under-treatment. As a result, there is an increased risk of opioid misuse, abuse, and overdose.

[17] Only 118 of the 150 patient records were subject to chronic opioid pain management requirements; the remaining 32 patients were not because they received prescriptions from a non-IHS provider (22 patient records) or their prescriptions were for the treatment of acute pain (10 patient records).

[18] We only determined whether more than 3 months had elapsed since the previous evaluation. We did not capture the number of months past the 3-month period that the next evaluation occurred.

[19] The training focuses on providing knowledge on several topics, including pain management, aberrant behaviors, risk factors, opioid treatments, non-opioid treatments, non-pharmacological treatments, and pain prevalence. The training must be completed every 3 years after completion of the initial training. The training is required for all Federal providers, contractors, clinical residents, and trainees.

Urine Drug Screenings Were Not Always Performed Within Recommended Time Intervals

The IHM requires that patients on opioids for pain management submit to both scheduled UDSs and unscheduled UDSs when providers' request them. UDSs are recommended at initiation of the treatment and periodically every 6 to 12 months thereafter, as appropriate. UDSs may be ordered by a provider during a hospital visit or by another healthcare professional (e.g., nurse or pharmacist) before opioids are dispensed (IHM 3.30.9.G). The UDS is favorable if the prescribed opioid is in the patient's sample. If the UDS is unfavorable, it can be either positive or negative. A UDS is positive when illegal substances are present in the UDS results and negative when the prescribed opioid is not present in the UDS results. If a UDS is positive, the primary or treating provider or a pain management team will take appropriate action (IHM 3.30.9.G).

At the five hospitals, we identified instances in which UDSs were not being performed within the recommended time intervals. Specifically, we found 27 out of 118 patients' records that did not show that UDSs had been performed every 6 to 12 months. For purposes of our testing, we only identified as errors patient records associated with patients who had gone more than 12 months without a UDS.[20]

From our patient record review, we also noted instances in which the patients' UDS lab results did not align with expected results and there was no evidence that the provider took action to follow up with the patient. For example, we noted UDS lab results for a patient that came back negative for the opioids prescribed, but there was no evidence in the patient's record that the provider had taken any action such as talking with the patient, the pain committee, or both, to determine whether opioid treatment should be continued. In another example, we noted UDS lab results for a patient that came back positive for recreational drugs, but there was no evidence of what the provider planned to do (e.g., retest the patient in a month or release the patient from the pain management agreement). In both of these examples, the hospital continued to prescribe and dispense opioids to the patients.

The five hospitals did not have mechanisms in place to alert providers when a patient was due for a UDS. In addition, the IHM does not define or provide examples of the type of action a provider should take or what documentation to include in the patient's EHR when the UDS is unfavorable. As a result, patients were at an increased risk for misuse of or addiction to prescribed opioids. At Phoenix, hospital officials told us that the hospital has since incorporated IT changes on the EHR to create an alert. The Phoenix officials further stated that the system alert addresses UDS, chronic opioid therapy (COT) expiration, PDMP monitoring, and patient education for pain management.

[20] We only determined whether more than 12 months had elapsed since the previous UDS. We did not capture the number of months past the 12-month period that the next UDS occurred.

Most of the IHS Hospitals We Reviewed Did Not Review Patient Health Records Before Filling a Prescription From a Non-IHS Provider

The IHM requires that a hospital pharmacist review the complete health record of each patient before dispensing medications. In contract community pharmacies,[21] patient medication profiles must be maintained and reviewed before dispensing medications. A complete review of the drug history and health record of each hospitalized patient must be conducted before the administration of medications when possible or as soon as a pharmacist is available. The standards of care developed or adopted by the professional staff of the facility are criteria for determining the appropriateness of drug therapy. Any concerns or questions identified during the pharmacist's review must be resolved with the provider before dispensing or administering any medication (IHM 3-7.3(B)).

Four of the five hospitals (Cass Lake, Fort Yates, Lawton, Phoenix) dispensed opioids from their pharmacies to patients with prescriptions from non-IHS providers without a pharmacist's review of the patient's medication profile, a complete drug history, or related health records. Out of 150 patient records we sampled from the five hospitals, 22 patient records indicated that patients were prescribed opioids by non-IHS providers and that those opioids were dispensed by the hospitals' pharmacies. For five patient records, the hospitals provided documentation received from the non-IHS provider, such as patient assessments and laboratory results. For the remaining 17 patient records, the hospitals did not provide evidence that the IHS hospital pharmacy staff had reviewed the patients' medication profiles, complete drug histories, or related health records before dispensing the medication. Also, there was no documentation in the patients' records from the non-IHS providers explaining why opioids were prescribed.

In reviewing patient records, we identified an instance in which one hospital (Fort Yates) refilled an opioid prescription from a non-IHS provider for a patient whose treatment was discontinued by an IHS provider for violating the pain management agreement. The area office responsible for overseeing that hospital identified a similar issue in its September 2017 pharmacy site survey report—a patient's opioid treatment was discontinued because the patient violated his or her COT agreement, but the treatment was restarted by a non-IHS provider and the opioid prescription was refilled at the Fort Yates pharmacy.

During our walkthrough at Fort Yates, the pharmacy staff requested a UDS on a patient who regularly refilled his or her prescription from a non-IHS provider at the hospital's pharmacy. When we asked if this was part of the hospital's normal operating procedures, we were told that it was not. The UDS lab result was unfavorable which indicated that the patient was not taking the prescribed opioid. The pharmacy called the non-IHS provider, who agreed that the opioid should not be dispensed.

[21] IHS may establish contracts with community pharmacies to provide pharmaceutical care for eligible patients. Community pharmacy contracts may be necessary in areas where there are no direct services available from IHS.

Officials at three of the four hospitals did not explain why they did not review patients' records before filling a prescription from a non-IHS provider. At the remaining hospital (Lawton), officials told us that patients who refill prescriptions from non-IHS providers at Lawton's pharmacy were not considered Lawton's "patients." However, we noted instances in which these patients were receiving other medical services (e.g., general, dental, and behavioral) at Lawton. Without proper monitoring of patients with prescriptions from non-IHS providers, there is an increased risk of opioid misuse or diversion.

Pain Management Documents Were Not Always Maintained To Support That Provider Responsibilities Had Been Performed

The IHM requires that patients sign an informed consent and COT agreement when the use of opioids for pain management can be reasonably clinically anticipated. Both the informed consent and the COT agreements must be signed within 60 days of the beginning of opioid use. Providers must use separate forms with separate signature acknowledgments for each. Informed consent addresses the risks, benefits, and alternatives for pain management (IHM 3.30.6.C). COT agreements outline the circumstances under which opioid pain medications may be initiated, used, and discontinued for pain management. COT agreements are also used to outline boundaries, expectations, and responsibilities of patients and providers, such as UDS and pill counts[22] (IHM 3.30.6.D). All COT agreements should be reviewed at least annually (IHM 3.30.6.C).

The IHM requires that providers convey to the patient that the safe and optimal management of pain is a primary goal of patient care and is consistent with the IHS mission and values. Patient education includes but is not limited to information about (1) the types of pain patients actually or potentially may experience, (2) available pain control mechanisms, (3) potential limitations of pain management and treatment, and (4) potential side effects of pain management treatment (IHM 3.30.8.A).

IHS hospitals did not always maintain pain management documents, including the informed consent and COT agreement, to support that the required pain management responsibilities had been completed, such as discussing risks, benefits, and alternatives to pain management and the requirement for UDS. Also, hospitals did not maintain evidence of patient education. Of the 118 patients' records we reviewed at the five hospitals:

- 105 patient records did not contain the informed consent;

- 90 patient records did not contain evidence that the provider educated the patients on the types of pain patients actually or potentially may experience;

[22] Pill counts occur when providers have a patient bring in his or her dispensed opioids to do a physical count. Based on our interviews, we determined that providers only do this when they suspect misuse by the patient.

- 89 patient records did not contain evidence that the provider educated the patient on pain control mechanisms available;

- 83 patient records did not contain evidence that the provider had educated the patient on potential limitations of pain management treatment;

- 79 patient records did not contain a COT agreement or evidence that an existing agreement had been reviewed annually;[23] and

- 77 patient records did not contain evidence that the provider had educated the patient on potential side effects of pain management treatment.

The IHM effective during our audit period did not specify that the informed consent and COT agreement be maintained in the patient's health record. The IHS hospitals, though, could not otherwise provide an informed consent and COT agreement for most of the patients associated with the sample of patient records that we reviewed. Also, the IHS hospitals did not have procedures in place describing how to document that patients had been educated on pain management treatment and did not have a system to ensure that the required documentation was maintained and provider responsibilities had been performed. The lack of specificity in the IHM and the lack of any tracking mechanism likely contributed to the high number of instances of missing documentation we identified.

Without maintaining essential pain management documents to demonstrate that provider responsibilities had been performed, neither we nor hospital management could determine whether providers were fulfilling their obligations to ensure patients were aware of (1) either the risks and benefits of or the alternatives to pain management treatment; (2) the risk of overdose associated with combining opioids with alcohol or recreational drugs; (3) their responsibilities outlined in the COT agreement, such as being subjected to a UDS and not taking other substances; and (4) what to expect from providers during pain management treatment.

After our site visits (in February 2018), IHS headquarters updated the IHM to require that the informed consent and COT agreement be maintained in the patient's health records but still did not have controls in place to ensure that the required documentation was maintained and provider responsibilities had been performed. An example of this is a tracking system or other mechanism that identifies (1) when the informed consent was signed; (2) when a COT agreement was initiated, updated, or annually reviewed; and (3) when patient education was provided regarding pain management.

[23] If there was evidence of a COT agreement but it was not annually reviewed, we considered this an error.

IHS HOSPITALS DID NOT FULLY USE THE STATES' PRESCRIPTION DRUG MONITORING PROGRAM WHEN PRESCRIBING OR DISPENSING OPIOIDS

On the basis of our interviews with hospital personnel and our review of a sample of patient records, we found that the hospitals (1) did not always update the PDMP with opioid dispensing data within required timeframes and (2) did not provide support that providers always checked the PDMP before prescribing or dispensing opioids. In addition, providers did not always perform PDMP monthly self-audits or provide a copy of the self-audits they did perform to their hospital's clinical director.

Hospitals Did Not Always Update the Prescription Drug Monitoring Program With Opioid Dispensing Data Within Required Timeframes

Each IHS area office must execute a memorandum of understanding (MOU) with the PDMPs in each State where an area office operates a pharmacy site (IHM 3.32.2.A & 3.32.2.C). This MOU must set forth the requirements for data disclosure to the State PDMP, including the frequency at which each pharmacy must report opioid dispensing data (IHM 3.32.1.C (5)). All Federal IHS pharmacy sites operating in a State with an MOU must ensure that dispensing data are reported at the frequency required by the MOU. Daily reporting is recommended to ensure a complete and accurate patient record (IHM 3.32.2.C).

Although three of the five IHS hospital pharmacies were reporting their opioid dispensing data daily, the remaining two (Fort Yates, Phoenix) were not—even though it is both recommended by IHS and required by the MOU with both States' PDMP (North Dakota and Arizona).[24] Fort Yates reported its data weekly and Phoenix reported its data Monday through Friday, even though the pharmacy was open 24 hours, 7 days a week. Hospital officials at Fort Yates told us they were not reporting data to the State PDMP daily because of limited staffing and the time it took to upload data that had to be done manually. Not reporting opioid dispensing data in a timely manner limits the effectiveness of PDMP data when it is checked by other providers. For example, a patient's complete history of opioid use may not be reflected in the PDMP, potentially allowing a patient to be prescribed opioids from multiple providers at the same time. As a result, there is an increased risk for patient harm or opioid misuse and diversion.

Hospitals Did Not Provide Support That Providers Always Checked the Prescription Drug Monitoring Program Before Prescribing and Dispensing Opioids

The IHM requires that providers must request a PDMP report as part of the process of accepting a new patient. This information can assist the provider with determining any possible

[24] Both States have issued guides that require daily reporting of opioid dispensing data: *North Dakota PDMP Data Submission Dispenser Guide*, March 2017; and *Arizona Controlled Substance Prescription Monitoring Program,* January 2017. Since the completion of our fieldwork, hospital officials from both Fort Yates and Phoenix informed us that they are currently in compliance with the requirement to report opioid dispensing data each day.

interactions among drugs or drug interactions with any prescribed therapy. This information can also help to identify recent doctor shopping.[25] To facilitate meaningful physician–patient interactions, providers must also access PDMP patient data before patient appointments. Providers should also review PDMP data when opioid prescriptions for acute pain exceed 7 days, when progressing from acute to chronic opioid pain therapy, and periodically during opioid therapy for chronic pain, ranging from every prescription to every 3 months (IHM 3.32.2.D). In addition, pharmacists must access PDMP data before processing an outside prescription for a controlled substance (IHM 3.32.2.E.1).

At each of the five IHS hospitals, we did not see evidence in some patient records that the provider had reviewed PDMP data before seeing new patients and every 3 months during opioid therapy for chronic pain. Specifically, we did not see evidence that the provider reviewed PDMP data before seeing a new patient in 60 of the 118 patient records. Additionally, we found that 68 of the 118 patient records did not have evidence to indicate that the provider reviewed the PDMP data every 3 months, as recommended by IHS. Further, for the 22 patient records related to opioids prescribed by a non-IHS provider, we did not see evidence at four of the five IHS hospitals that pharmacy staff reviewed PDMP data before processing the patients' outside prescriptions for opioids.

The five IHS hospitals did not have processes to document that providers and pharmacists checked PDMP data. A provider at one hospital told us that, because of the large number of patients, he did not want to take the time to review the PDMP data. Evidence in patient records of PDMP data checks allows hospital management to be assured that providers and pharmacists are assessing patients' opioid use. As a result, there is an increased risk for patient harm, opioid misuse, and diversion.

Providers Did Not Always Perform Prescription Drug Monitoring Program Monthly Self-Audits or Provide Copies of Them to the Hospital Clinical Director

The IHM requires that the IHS Area Director ensures the PDMP MOU is current, signed, and archived as required by the MOU and as allowable by State law (IHM 3.32.2A). Providers must register with State PDMPs and must perform self-audits monthly and send a copy of the self-audit's report to the hospital's clinical director (IHM 3.32.2.D). Providers perform self-audits to verify that details about dispensed opioids reported in the PDMP database under the provider's name are accurate.

[25] The term "doctor shopping" has traditionally referred to a patient obtaining controlled substance prescriptions from multiple healthcare practitioners without the providers' knowledge of the other prescriptions: https://www.cdc.gov/phlp/docs/menu-shoppinglaws.pdf. Accessed on October 5, 2018.

Through our interviews at each of the five IHS hospitals,[26] providers at two hospitals (Phoenix and Northern Navajo) told us they performed self-audits monthly. We confirmed this by seeing copies of provider self-audit reports. At another hospital (Lawton), a provider told us self-audits were completed periodically but was not certain if they were completed monthly. At the remaining two hospitals (Cass Lake and Fort Yates), providers told us they did not perform self-audits of the PDMP data.

In addition, during our interviews with the clinical director[27] at the three hospitals with providers who performed self-audits, we learned that the providers at two hospitals (Phoenix and Northern Navajo) sent a copy of the self-audits to their clinical directors, but providers at the other hospital (Lawton) did not. At Phoenix, the clinical director told us that providers sent a copy of self-audits to her every 6 months but not monthly as required by the IHM. At Northern Navajo, the self-audits are first given by the providers to the Quality Assurance Officer, who then sends a monthly report to the clinical director. The clinical director provides the monthly report to Northern Navajo's Chronic Pain Committee and the Peer Review Committee for review. The Chronic Pain Committee reviews the self-audit reports to identify issues such as patients who (1) were prescribed both opioids and benzodiazepines and (2) had outside narcotic prescriptions. The Chronic Pain Committee then sends a letter to the provider highlighting any concerns. The Peer Review Committee records the submission of the self-audits on the provider's professional practice evaluation, which is reviewed by the credentialing committee at reappointment. The submission of self-audits to a hospital committee for review is an effective way to ensure required self-audits are performed and thereby confirming the accuracy of the PDMP data.

At Lawton, where the self-audits were completed periodically but not necessarily monthly, the clinical director told us that, for legal reasons, a copy of the self-audits could not be sent to the clinical director. The clinical director also stated that IHS headquarters was aware of that situation. From our review of the MOU between Lawton and Oklahoma, however, we determined that the issue is not that providers may not provide copies of self-audits to the clinical director but that providers may not access PDMP to conduct self-audits. According to the MOU, providers may only access the State PDMP in situations that relate to patient care. This MOU restriction conflicts with the IHM requirements.

Without access to providers' monthly self-audits, hospital management cannot determine whether the staff are complying with the IHM requirements to (1) register with the State PDMP and (2) review the PDMP data before prescribing opioids. For example, at Fort Yates, where

[26] At each of the five IHS hospitals, we interviewed a provider regarding their duties to perform PDMP self-audits monthly.

[27] At each of the five IHS hospitals, we interviewed the clinical director who is supposed to receive the PDMP self-audits monthly from the providers.

providers do not perform monthly self-audits, a provider was not registered with the State PDMP but was prescribing opioids to patients.[28]

IHS HOSPITALS DID NOT ALWAYS ENSURE OPIOIDS WERE PHYSICALLY SECURE

The IHM requires that opioids be stored in a substantially constructed locked cabinet, safe, or drawer (IHM 3-7.3(D)(2)(a)(xii)(c)(i)(a)).

We observed some effective physical security controls during our on-site visits at the five IHS hospitals. For example, we noted that cameras were located inside and outside of pharmacies (Appendix B, Figures 10 and 11), entrances to the pharmacies at all five hospitals required either a badge or a personal identification number (Appendix B, Figure 12), visitors were required to sign in when entering the pharmacy and computer rooms, and computer server rooms required a badge to gain access (Appendix B, Figure 13).

But during our walkthroughs of the five IHS hospital pharmacies, we observed that only Lawton stored its dispensed opioids that are waiting for patient pickup in a secured storage cabinet that requires employee authentication to access.[29]

The remaining four hospitals (Cass Lake, Fort Yates, Phoenix, Northern Navajo) did not always ensure that opioids were physically secure. During our walkthroughs at these hospitals, we observed the following situations during pharmacy operating hours:

- dispensed opioids for discharged patients were not locked in a cabinet or safe (Phoenix),
- dispensed opioids awaiting patient pickup were left out in the pharmacy with other non-opioid prescriptions (Cass Lake),
- opioids were held in an unlocked cage (Fort Yates), and
- opioids were stored in a separate room with a door that was not always locked (Northern Navajo).

At Phoenix, officials stated they do not have the space to hold opioids in a locked safe or cabinet. At Cass Lake, an official stated that it was the hospital's practice to mix opioids with

[28] Hospital management told us that they were aware the provider was not registered but was in the process of registering. This provider has since registered with the State PDMP. Fort Yates later provided us with supporting documentation from the State PDMP verifying this provider was registered.

[29] These secure cabinets store dispensed opioids that are waiting for pickup in the pharmacy. To retrieve the prescription, clerks must enter a few letters of the patient's name into a computer, and the system then lights the correct drawer and compartment. Lights and sounds confirm that clerks have selected the correct prescription and warn when the clerks pick the wrong one. If an unauthorized employee attempts to access the cabinet, an alarm will sound. One example of a secure storage cabinet used in many pharmacies is the Intellicab.

other medications to avoid "singling patients out" when they pick up their prescriptions. The Cass Lake official told us that, in the past, Cass Lake had issues with patients waiting in the lobby and following other patients out of the hospital to steal their opioids. The official said that because the patients waiting in the lobby could tell where the opioid was being dispensed, they could easily identify which patients were picking up opioid prescriptions. At Fort Yates, an official stated that many of the pharmacists go in and out of the cage, so it was easier to leave it open during business hours but that the cage was locked at close of business. At Northern Navajo, an official stated that the pharmacy has compensating controls in place, such as limiting pharmacy access to only pharmacy personnel.

Not securing controlled substances in a locked cabinet, safe, or drawer increases the risk of theft or diversion of opioids.

IHS HOSPITALS DID NOT ALWAYS USE AVAILABLE DATA TO IDENTIFY RISKS IN THEIR PRESCRIBING AND DISPENSING PRACTICES

The Government Accountability Office states that effective information and communication are vital for an entity to achieve its objectives. Management should use quality information to achieve the entity's objectives and should internally communicate the necessary quality information to achieve those objectives.[30]

IHS's Quality Framework states that to provide patient-centered, timely, effective, safe, and reliable healthcare of the highest quality, IHS will incorporate data-supported decision making.[31] IHS has also said that data analysis and management will be crucial to identifying risks and taking action to reduce occurrence of adverse events.[32]

CDC's *Guideline for Prescribing Opioids for Chronic Pain* states that scientific research has identified high-risk prescribing practices that have contributed to the overdose epidemic (e.g., prescribing high doses, overlapping opioid and benzodiazepine prescriptions, and extended-release/long-acting opioids for acute pain). According to CDC, using guidelines to address

[30] Government Accountability Office; *Standards for Internal Control in the Federal Government*; "Control Activities," p. 46; and "Information and Communication" p. 58; Sept. 2014.

[31] The IHS Quality Framework describes the vision, goals, and priorities to develop, implement, and sustain an effective quality program that improves patient experience and outcomes, strengthens organizational capacity, and ensures the delivery of reliable, high quality healthcare for IHS Direct Service facilities (https://www.ihs.gov/newsroom/includes/themes/newihstheme/display_objects/documents/IHS_2016-2017_QualityFramework.PDF, accessed August 16, 2018).

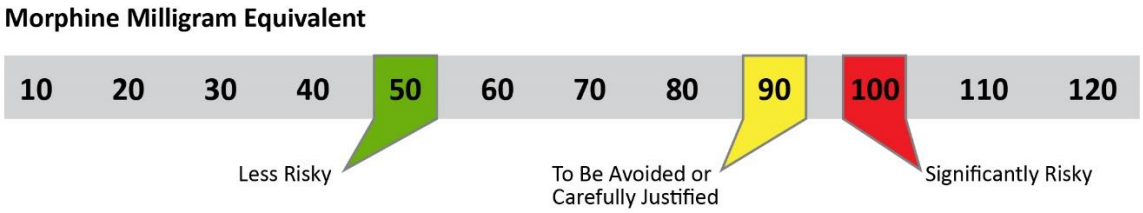
[32] https://www.ihs.gov/newsroom/factsheets/nationalqualityaccountability/. Accessed April 17, 2018.

problematic prescribing has the potential to improve care and patient safety.[33] Relevant recommendations in the guideline are as follows:[34]

- When opioids are started, clinicians should prescribe the lowest effective dosage. Clinicians should use caution when prescribing opioids at any dosage, should carefully reassess evidence of individual benefits and risks when considering increasing the dosage to 50 or more MMEs per day, and should avoid increasing the dosage to 90 or more MMEs per day. Experts also noted that daily opioid dosages close to or greater than 100 MMEs per day are associated with significant risks (Figure 6).

- Before starting and periodically during opioid therapy, clinicians should evaluate risk factors for harm related to opioid use. Clinicians should incorporate into the management plan strategies to mitigate risk, including considering offering naloxone[35] when factors that increase risk for opioid overdose, such as concurrent use of benzodiazepines, are present.

Figure 6: Graphic Representation of CDC Guidelines for Daily Morphine Milligram Equivalents



Although all five IHS hospitals maintained prescribing and dispensing data, some hospitals did not use the available data to identify potential risks in its prescribing and dispensing practices, such as opioid dosages equal to or greater than 90 MMEs per day or patients who had been prescribed both opioids and benzodiazepines at the same time.[36] In addition, four of the five IHS hospitals (Cass Lake, Lawton, Phoenix, Northern Navajo) did not maintain readily available

[33] 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 5, 2018.

[34] The IHM did not include the CDC recommendations when we started our audit; however, in February 2018, these recommendations were included in the updated IHM Part 3, chapter 30. Also, see "Figure 1: Efforts to Combat the Opioid Epidemic" in the Background section of this report.

[35] Naloxone is a medication approved by the Food and Drug Administration to prevent overdose by opioids such as heroin, morphine, and oxycodone. (https://www.samhsa.gov/medication-assisted-treatment/treatment/naloxone. Accessed February 20, 2019.

[36] During our site visits at four hospitals, we observed pain management meetings to discuss patient opioid treatment. Three hospitals showed us reports of their opioid data analyses; however, only two of the hospitals used those reports during pain management meetings. On the basis of our interviews and review of the documents provided, we determined that hospitals did not start analyzing the data available to them until July 2017.

data on opioid prescriptions that were dispensed by a pharmacy not affiliated with the IHS hospital.

We obtained and analyzed from the five IHS hospitals data from August 1, 2016, to July 31, 2017, on dispensed opioids and found that all five hospitals had patients who were dispensed opioids in amounts that exceeded CDC's guidelines. The data on dispensed opioids that we analyzed included opioids dispensed to both cancer and non-cancer patients.[37] At each hospital, we identified patients who were prescribed and dispensed opioids at dosages of over 90 MMEs per day. At one hospital (Northern Navajo), the opioid dosage was as high as 500 MMEs per day. Also, at all five hospitals, we found that some patients were prescribed opioids and benzodiazepines at the same time. Per CDC guidelines, concurrent use of opioids and benzodiazepines puts patients at greater risk of a potentially fatal overdose.

Hospitals did not effectively track all opioids prescribed by their providers in the patient records, including opioids dispensed by an outside pharmacy. We requested prescription data for opioids prescribed by IHS providers but filled at outside pharmacies for FY 2013 through 2017. One hospital (Fort Yates) had no data because the hospital pharmacy filled all prescriptions written by any providers at the hospital. The data provided by the other four hospitals varied. Phoenix provided data for our request, but these data also included medications prescribed by non-IHS providers and was based on information gathered from the patients and noted in their records. Three of the hospitals provided some prescription data but were unable to provide data that covered the entire timeframe of our request. Lawton provided outside prescription data for the period starting June 2016. Lawton was able to retrieve this information because of a secure prescription printing software it installed in June 2016 that allowed providers to print prescriptions from the patient's EHR instead of handwriting them. The other two hospitals (Cass Lake[38] and Northern Navajo) were able to retrieve the prescription data only by reviewing PDMP provider reports, which contain information on the type of controlled substances, the dosages of those substances, the provider's name, and the location where these prescriptions were filled. However, they were unable to provide data for entire period of our request.

The intent of our data analysis was to highlight ways in which hospitals might use existing opioid data to identify risks in opioid prescribing and dispensing practices. Making data-supported decisions requires the use of analysis to reassess current treatments and consider if alternative treatment methods (such as physical therapy) could be used for chronic non-cancer pain management. As hospitals continue to implement the CDC opioid-prescribing guidelines, which have now been integrated into IHS policy, it will be important that hospitals use existing

[37] Hospital officials told us the available data on dispensed opioids could not readily be separated by whether that patient has cancer or not. The CDC guideline recommendations are for primary care clinicians who prescribe opioids for chronic pain outside of cancer treatment, palliative care, and end-of-life care. The data we analyzed included both types of patients and may overstate risks.

[38] In gathering this data for our audit, Cass Lake identified two providers who wrote prescriptions that were not recorded in the patients' records. Cass Lake referred the two providers to OIG's Office of Investigations.

resources and data to mitigate risks of harm to patients and ensure compliance with IHS requirements.

IHS AREA OFFICES DID NOT ALWAYS PERFORM REQUIRED HOSPITAL REVIEWS

The Headquarters IHS Chief of Pharmacy Services is responsible for the oversight, support, and evaluation of area pharmacy programs, including the evaluation of area quality improvement activities (IHM 3.7.2.A (1)(d)). The Area Pharmacy Officer (APO) is responsible for conducting annual reviews of all service unit pharmacy programs in his or her area (IHM 3.7.2.A (2)(c)). The APO or a designee must conduct an annual physical audit of all Schedule II controlled substances at each facility in the area. All Schedule II controlled substances must be audited and the count verified against the inventory records. Every location in the facility where controlled substances are maintained must be randomly audited for accuracy, discrepancies, and compliance with controlled drug procedures (IHM 3.7.3.D (2)(a)(xii)(bii)(d)).

IHS area offices did not perform all of the required annual pharmacy program and Schedule II controlled substance reviews. We found that when area offices completed the required annual reviews, not all area offices reported the same results or included the same level of detail in their reports. The IHM does not specify the topics to be included in these annual reviews. In addition, the IHM does not require that these reviews be submitted to IHS headquarters.

Four of the five hospitals (Fort Yates, Lawton, Phoenix, and Northern Navajo) provided us with documentation supporting what they considered to be the annual review of pharmacy programs. The remaining hospital (Cass Lake) did not provide any documentation that it had performed an annual review of its pharmacy program. On the basis of our review of the four hospitals' documentation, we determined that only two of hospitals (Phoenix, Northern Navajo) met the requirement for conducting a pharmacy program review. However, the two reviews did not cover the same areas. For the remaining two hospitals (Fort Yates, Lawton), we determined that the documentation did not demonstrate that their reviews met the requirements for conducting a pharmacy program review. Specifically, Lawton's and Fort Yates' documentation comprised excerpts from a mock survey[39] that was performed to identify areas of improvement or deficiencies before the facility underwent accreditation. Mock surveys are performed for a different purpose, and the IHM does not indicate that a mock survey can be substituted for a pharmacy program review. See Table 1 for a summary of the areas covered by pharmacy program reviews conducted at the five hospitals.

[39] A mock survey typically includes methods similar to those that CMS uses during hospital certification surveys or that accrediting organizations use during hospital accreditation surveys. These methods include direct observations, policy reviews, and medical record reviews.

Table 1: Pharmacy Program Reviews at Five IHS Hospitals

	Cass Lake	Fort Yates	Lawton	Phoenix	Northern Navajo
Date of last program review	None	None	None	11/15/16	10/11/16
Review submitted to IHS HQ	No	No	No	No	No
Areas Included in Review					
Physical security of controlled substances	No	No	No	Yes	No
PDMP dispensing data reported to the State	No	No	No	Yes	Yes
Recommendations for improvement	No	No	No	Yes	No

All five hospitals had Schedule II controlled substance audits and provided us their audit reports. However, we noted that the IHS area offices did not conduct the audits annually, as required. For example, we found one hospital (Cass Lake) for which the area office had not performed the Schedule II controlled substance audit since 2011. In addition, we found that the audits varied regarding areas reviewed, level of detail, and format. Table 2 provides a summary of the areas covered by the most recent Schedule II controlled substance audits performed at the five hospitals.

Table 2: Controlled Substance Audits at Five IHS Hospitals

	Cass Lake	Fort Yates	Lawton	Phoenix	Northern Navajo
Date of last controlled substance audit	11/28/11	9/12/17	8/15/17	11/29/16	11/16/17
Audit completed for the last 3 years	No	No	Yes	No	Yes
Areas Included in Audit					
Review of patient records	No	Yes	No	Yes	No
Controlled substance policies	Yes	Yes	Yes	Yes	No
Pharmacy ordering practices	Yes	Yes	Yes	Yes	No
Physical security of controlled substances	Yes	Yes	Yes	Yes	Yes
PDMP dispensing data reported to State	No	No	No	Yes	Yes
Recommendations for improvement	Yes	Yes	Yes	No	Yes

IHS area office officials told us that the reviews were not always completed annually because they did not have adequate staff to complete them and that many employees were acting in multiple positions. For example, at one hospital (Cass Lake), an APO was acting as the Hospital Lead Pharmacist (and therefore lacked the independence needed to perform the review), but the hospital did not invite another area office to independently perform the audit. At another hospital (Phoenix), officials told us that no audits were conducted between 2011 and 2016 because of a prolonged vacancy in the APO position.

The audits did not all cover the same areas because the IHM does not specify the areas to be included in these annual reviews. In addition, the IHM does not require that these reviews be submitted to IHS headquarters. Accordingly, IHS headquarters may not be aware of concerns identified during the annual reviews. If IHS headquarters does not review the same areas at all hospitals, it is less likely to identify any best practices and opportunities for improvement across the hospitals. Further, if the area office reviews are not performed in a timely manner and consistently, control weaknesses in prescribing and dispensing opioids may not be identified and, in turn, hospitals would not know what corrective actions may be needed to improve hospital operations.

IHS HOSPITALS' SECURITY CONTROLS TO PROTECT HEALTH INFORMATION AND ENSURE PATIENT SAFETY COULD BE IMPROVED

During our reviews, we identified common IT vulnerabilities, which contributed to an insecure and unstable IT environment. The IT vulnerabilities existed primarily because the IHS hospitals did not always follow Federal requirements. The IT vulnerabilities also occurred because of the decentralized structure of IHS and an inconsistency in the delivery of cybersecurity services among IHS area offices and hospitals. This decentralization contributed to inconsistent patching, monitoring, and IT functions. IHS should consider addressing these systemic weaknesses by centralizing its IT functions and management, which can be done in a phased approach.

We identified the following vulnerabilities based on our review of IT security controls at the five hospitals:

- Patch management processes were inadequate to ensure that critical patches were installed in a timely manner at all five hospital we reviewed. None of the five hospitals had follow-up procedures for ensuring that patches were installed within required timeframes.

- Unsupported or end-of-life network equipment remained in use without extended service support contracts at four hospitals.

- While we observed some effective physical security controls in place at the four hospitals (Appendix B, Figures 10 through 13), we also observed some physical security controls that were not in place (Appendix B, Figures 7 through 9).

- There were inadequate contingency plans for information systems at four hospitals as part of an overall organizational program for achieving continuity of operations for mission and business functions, and one hospital did not have a contingency plan.

- Risk assessments were not adequate at all five hospitals; the assessments did not include all IT assets, which may have affected the integrity and availability of all of its critical healthcare systems.

- Flaw remediation at all five hospitals was inadequate to ensure all devices were scanned and vulnerabilities remediated.

- Some hospitals did not maintain secure wireless network configurations, and four hospitals either did not conduct wireless scans for unauthorized (or rogue) access points or did not always investigate unauthorized access points.

- The five IHS hospitals had ineffective controls to prevent or detect cyberattacks. We identified common vulnerabilities at multiple hospitals. The likely level of sophistication needed to exploit and compromise the IHS systems we tested is low, as the attacks did not require significant technical knowledge.

In a supplement to this report, we have provided more detailed information and specific recommendations to IHS so that it can address specific vulnerabilities that we identified. The recommendations include actions that IHS should take now to address the vulnerabilities we identified in addition to considering centralizing its IT functions and management.

Based on the results of our testing of IT controls, we scored each hospital in Table 3. We provided detailed findings and recommendations separately to IHS.

Table 3: Hospital Scores Based on IT Controls

Control	Case Lake	Fort Yates	Lawton	Phoenix	Northern Navajo	Average
Patch management	3	3	2	2	2	2
System and service acquisition	5	4	4	3	3	4
Physical access	4	2	3	3	4	3
Contingency planning	2	1	2	2	3	2
Risk assessments	3	3	2	3	3	3
Flaw remediation	3	3	2	2	2	2
Wireless network administration	4	4	4	3	3	4
Configuration management	4	3	3	4	4	4
Logical access	4	1	1	3	3	2

Hospital Scoring Criteria (based on IHS and National Institute of Standards and Technology (NIST) regulations and guidance – see Appendix D)

1. No control was in place.
2. Control was in place but deemed insufficient or ineffective.
3. Control was in place and was moderately effective.
4. Control was in place and effective; only minimal areas for improvement.
5. Control was in place and highly effective; no improvements recommended.

IT vulnerabilities that exist across IHS hospitals jeopardize patient care and hospital operations; stable and secure IT operations allow providers to be more effective in their healthcare functions. IHS's decentralized IT management structure increases the risk of a cybersecurity incident that could jeopardize IHS's ability to serve and protect its user population.

Strategic change will be required to foster modifications in the way IHS delivers cybersecurity and IT services to its hospitals. Centralization, including the use of cloud, could result in enhanced cybersecurity controls at all 25 IHS hospitals. Benefits of centralization include potential cost savings and reduced burden on hospital IT staff and IHS management. Operating 25 disparate networks is challenging. We have observed that most private sector and Government organizations have concluded that the 1990's model of local network administration, results in enhanced cybersecurity risks and increased costs and negatively

affects resiliency. Significant changes in the administration of IT assets would also result in modifications within IHS's IT management structure. Changes can be implemented in a phased approach. Conversely, some organizations conduct risk assessments and conclude that because of the type of data they possess and the missions of their organizations, decentralization is the best solution and they are willing to accept the associated risks and challenges.

We discussed with IHS senior officials the possibilities that cloud services could provide enhanced security and resiliency. OIG does not endorse one cloud solution or provider over another and cannot guarantee that moving to a cloud environment will resolve all IT vulnerabilities. Correction of longstanding weaknesses will also require significant changes in culture, accountability, and vision.

RECOMMENDATIONS

We recommend that IHS:

- revise the IHM to:
    - include the type of action a provider should take and what documentation to include in the patient's EHR when a UDS is unfavorable;
    - require area offices to submit completed annual reviews to IHS headquarters; and
- increase oversight of IT systems by IHS management, including consideration of centralizing its key IT systems (including RPMS), services, and cybersecurity functions (e.g., patch management, unsupported network equipment and contingency planning) by conducting a cost-benefit analysis and risk assessment of adopting the Cloud First Policy and other means of centralization (e.g., headquarters, area offices). Specifically, determine if a cloud solutions or other modernization approaches are most effective and cost efficient in addressing persistent cybersecurity vulnerabilities and increasing network resiliency.
- present findings and cost savings analysis to tribal leadership and the IHS user community to get buy-in for any significant IT enterprise changes.
- implement a strategic and phased approach to centralization of IT systems, services and cybersecurity functions.

We recommend that IHS work with hospitals to:

- ensure pain management and related documentation is done in accordance with IHS policies and procedures;

- develop policies and procedures to review the EHRs of patients with opioid prescriptions from non-IHS providers and document the results of the review in the EHR, particularly for those patients who had previously violated their COT agreements;

- ensure opioid dispensing data are complete, accurate, and submitted in a timely manner to the State PDMP for use by providers and pharmacists;

- ensure all opioids are in a locked cabinet, safe, drawer, or other appropriate secure container at all times;

- track all opioids prescribed at the hospital in the patient EHRs, including those being filled at an outside pharmacy;

- analyze opioid data to make decisions and oversee providers to minimize prescribing practices that exceed daily MME guidelines established by IHS, co-prescribe opioids and benzodiazepines, and use opioids for acute pain; and

- remediate the IT vulnerabilities identified.

We recommend that IHS work with area offices to:

- renegotiate the MOU with Oklahoma and other States that have restrictive MOU language to allow for PDMP self-audits and collection by clinical directors; and

- complete required annual reviews that are consistent in type and level of detail across all IHS hospitals.

IHS COMMENTS

In written comments on our draft report, IHS concurred with our recommendations and described actions that it had taken or plans to take to implement them.

IHS's comments are included as Appendix E.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We limited our review to IHS's implementation of certain internal controls. We judgmentally selected these hospitals based on each being located in different area offices, the number of opioids that the hospitals dispensed, the percentage of increase in opioids dispensed from FYs 2013 through 2016, and the number of opioids dispensed per user for FYs 2013 through to 2016. For this audit, we reviewed IHS's opioid prescribing and dispensing practices and information system controls at five IHS hospitals in the following areas:

- prescribing and dispensing of opioids
- patch management
- configuration management and system and services acquisition
- physical security
- contingency planning
- risk assessments
- flaw remediation
- wireless network configuration
- logical access

We contracted with DPS to conduct penetration tests at the five IHS hospitals. DPS provided subject matter experts throughout the testing. We closely oversaw DPS's work to ensure that testing was performed in accordance with government auditing standards. The penetration testing covered all Internet Protocol address ranges provided by IHS that were registered to or owned by IHS for the five IHS hospitals under review. We did not review IHS's overall internal controls. Our detailed observations are specific to the five IHS-operated facilities that we visited. We conducted our fieldwork at the five hospitals as follows:

- Cass Lake Hospital, Cass Lake, Minnesota, from August 28 through September 1, 2017;
- Fort Yates Hospital, Fort Yates, North Dakota, from September 25 through 29, 2017;
- Lawton Indian Hospital, Lawton, Oklahoma, from October 16 through 20, 2017;

- Phoenix Indian Medical Center, Phoenix, Arizona, from November 13 through 17, 2017; and

- Northern Navajo Medical Center, Shiprock, New Mexico, from December 11 through 15, 2017.

METHODOLOGY

To accomplish our objectives, we:

- reviewed the IHM and hospital policies and procedures;

- interviewed hospital staff using questionnaires to gain an understanding of hospital-specific policies and procedures for prescribing and dispensing opioids;

- assessed IHS and hospital policies and procedures for applicable audit areas;

- performed a walkthrough of each hospital pharmacy;

- judgmentally selected 150 patient records (30 patients records from each of the 5 hospitals) with opioid dispensed dates of August 1, 2016 through July 31, 2017, and tested for compliance with the IHM,[40]

- analyzed data for opioids dispensed during FYs 2013 through 2017 at these hospitals to identify opioid prescribing patterns and anomalies;

- reviewed audit reports prepared by area offices on Schedule II controlled substances;

- reviewed reports prepared by area offices on pharmacy program reviews;

- reviewed pharmacy inventory reports for completeness and accuracy;

- reviewed applicable Federal regulations, NIST guidance, and industry best practices for IT;

- interviewed appropriate computer operations personnel who were responsible for information security;

- analyzed system configuration reports for potential network vulnerabilities;

- performed an internal penetration test at each hospital; and

[40] Our sample did not include records associated with patients who were undergoing cancer treatment.

- discussed our findings with IHS officials.

We shared information about our penetration test findings with IHS following the tests and informed IHS about other preliminary findings before issuing our draft report.

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.

APPENDIX B: PHOTOGRAPHIC EXAMPLES

Figure 7: Live network ports in an open area at a hospital that could be used to access the hospital's computer network.

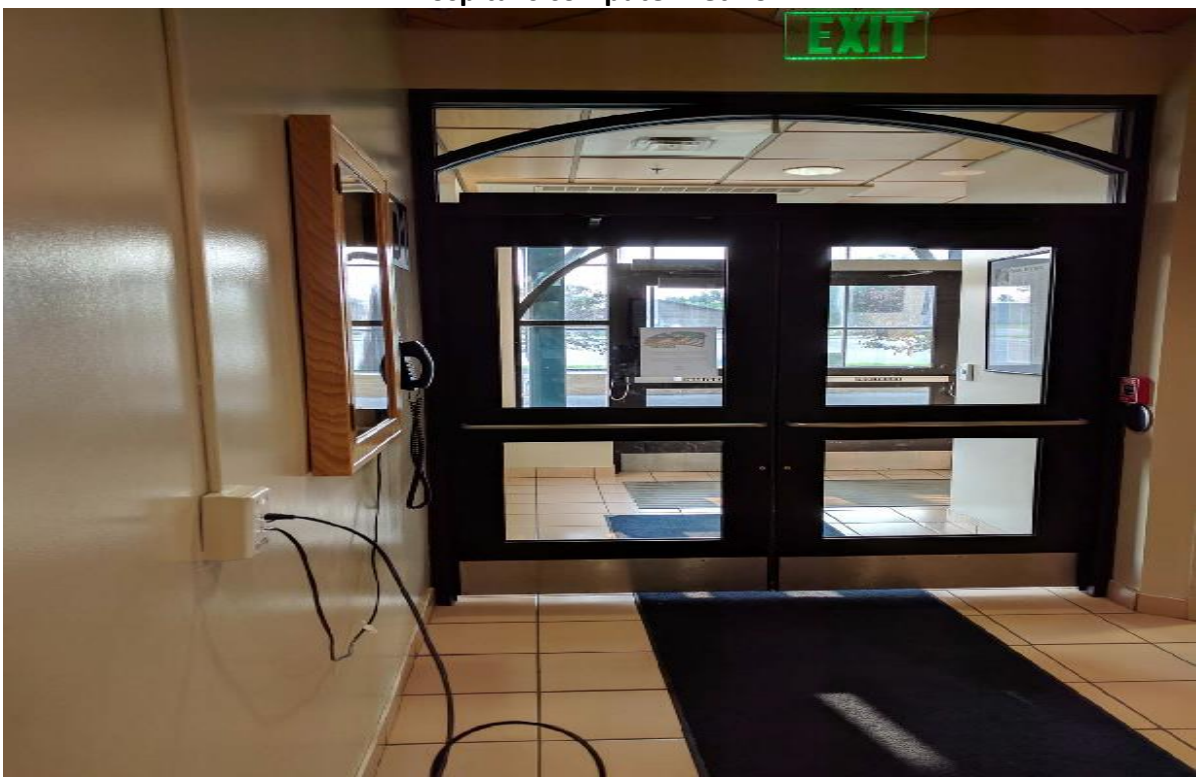


Figure 8: Unsecured electrical panel in a hallway.

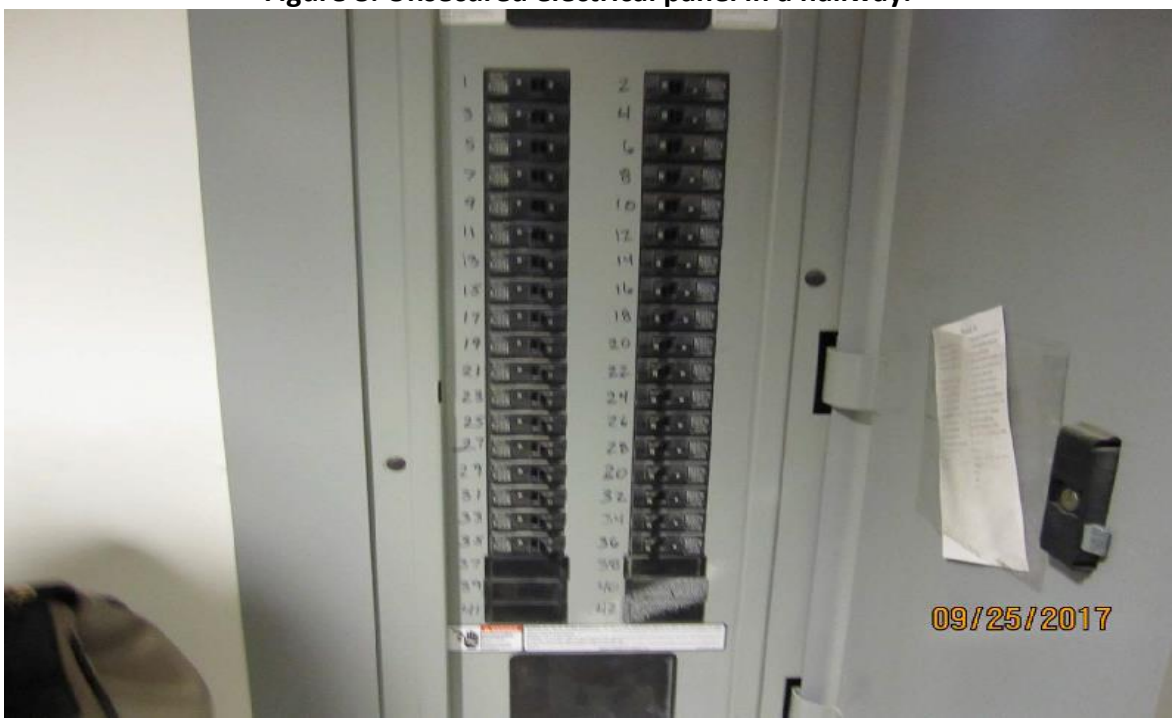


Figure 9: Controlled substances safe with combination on front of the safe.

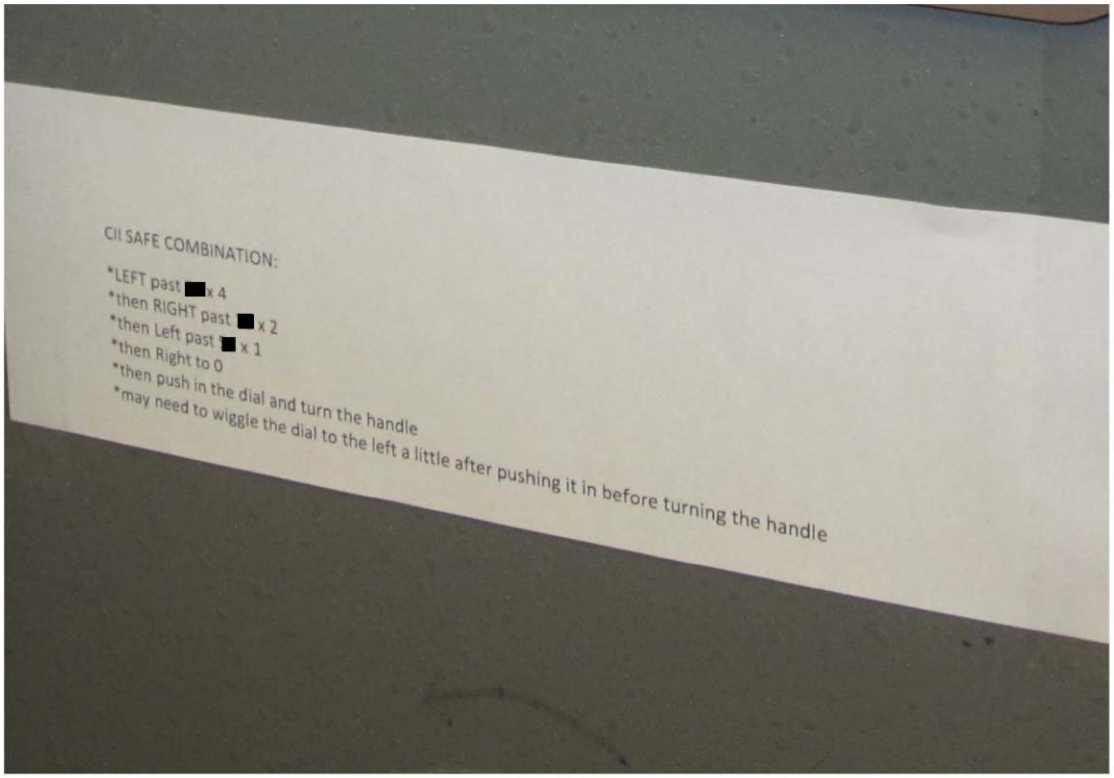


Figure 10: Cameras monitoring areas of the hospital.

Figure 11: Cameras in the pharmacy.

Figure 12: Entrance to the secured pharmacy area requires a badge for access.

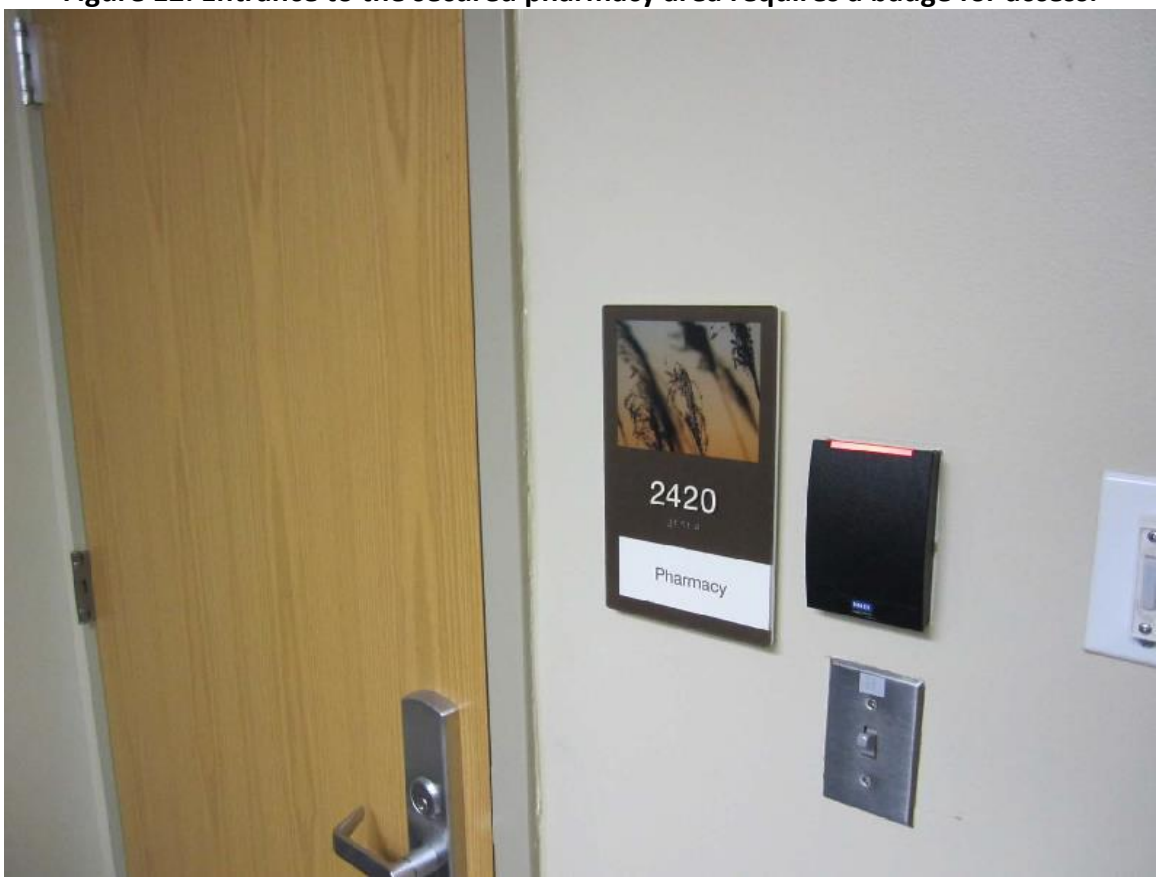


Figure 13: Entrance to the secured computer server room requires a badge for access.

APPENDIX C: DETAILS OF PATIENT RECORD FINDINGS

Table 4: Details of Patient Record Findings by Location

Documentation	Cass Lake		Fort Yates		Lawton		Northern Navajo		Phoenix		Total		
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	ALL
Proof the patient's treatment was reviewed at least every three months	17	4	11	10	21	3	26	4	13	9	**88**	**30**	**118**
Proof of UDS	19	2	18	3	20	4	14	16	20	2	**91**	**27**	**118**
Copy of Informed Consent	0	21	1	20	6	18	0	30	6	16	**13**	**105**	**118**
Copy of COT Agreement	14	7	10	11	7	17	2	28	6	16	**39**	**79**	**118**
Proof that patient education related to the types of pain patients actually or potentially may experience was provided	8	13	0	21	3	21	10	20	7	15	**28**	**90**	**118**
Proof that patient education related to pain control mechanisms available was provided	9	12	0	21	4	20	10	20	6	16	**29**	**89**	**118**
Proof that patient education related to the potential limitations of pain management and treatment was provided	14	7	0	21	3	21	12	18	6	16	**35**	**83**	**118**
Proof that patient education related to potential side effects of pain management treatment was provided	17	4	0	21	5	19	12	18	7	15	**41**	**77**	**118**
Proof that PDMP was accessed before the patient saw the doctor	1	20	6	15	11	13	25	5	15	7	**58**	**60**	**118**
Proof that PDMP was accessed every 3 months, prior to reissuing or refilling for a chronic controlled substance prescription for Schedules CII-CV medications	1	20	7	14	8	16	26	4	8	14	**50**	**68**	**118**

APPENDIX D: FEDERAL REGULATIONS AND GUIDANCE FROM THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

FEDERAL REGULATIONS

HHS Policy

The HHS *Information Systems Security and Privacy Policy* (pages 32, 91, and 92) states that the organization must develop a plan of action and milestones (POA&M) to ensure that system weaknesses are captured and their status updated in accordance with the HHS standard. The POA&M should include remedial actions proposed to correct identified weaknesses and to reduce or eliminate known system vulnerabilities.

Indian Health Manual

The IHM, 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 IHM, section 8-12, "Information Technology Security," 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. The Area Information Systems Security Officer should ensure contingency and disaster recovery plans are developed for all sensitive IT systems within each operating unit.

Section 8-12.1H(2)(b), "Contingency Planning," states:

> 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.

Section 8-12.1H(1)n(i) "Risk Management Process" states that: "All IHS organizations shall establish and implement a risk management process for all IT resources to ensure the balance of risks, vulnerabilities, threats, and countermeasures achieves a residual level of acceptable risk. The acceptable level of risk is based on the sensitivity or criticality of the individual systems."

Section 8-12.1G(7)(h) states that it is the responsibility of the Area Information Systems Security Officer to ensure that "a risk analysis is completed for all sensitive IT systems within the operating unit."

Section 3-7.3D (xii)(c),(i) (a-b) "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.

IHS Manual 3-7.3(D)(2)(a)(v) states that "Prescriptions resulting from patient visits to a non-contract practitioner or to a contract provider without prior IHS referral may be filled by the IHS or at IHS expense only if the drug is included in the facility's formulary and is in stock. A more restrictive policy may be established by each Area Director and shall apply Area-wide."

Indian Health Service Standard Operating Procedures

IHS Office of Information Technology, *Standard Operating Procedure for Enterprise Patch Management*, DITO-SOP-13-2, version 1.2, 3. "Roles and Responsibility for Patch Management" (pages 5 and 6) states that enterprise IT must test all critical patches against standard supported IHS applications and operating systems within 3 business days after vendor release and ensure availability of approved critical patches to areas or facilities within 5 business days of vendor release. Also, the area Information System Security Officer must test all critical security patches against local standard system configurations within 3 business days of deployment to a local site server and deploy all critical patches to all supported workstations and servers within 10 business days of availability to a local site server.

IHS Division of Information Security, *IHS Technical and Managerial Security Handbook*, DIS-SOP-06-11b, 4.7.2, "Patch Management" (page 33) states that "All patching must occur within 14 calendar days from the date that the patch or update is released. This may require the establishment of a maintenance window to allow for the reboot of critical systems during non-peak hours."

IHS Division of Information Security, *Standard Operating Procedure for General User Security Handbook*, DIS-SOP-06-11a, version 2.4, 10.1.1, "Visitor Procedure" (pages 39 and 40) states:

> Visitor control provides accountability for the movements of visitors within a facility. Without proper controls in place, visitors may be able to gain access to sensitive data, systems, or processing areas.
>
> Procedures
>
> - Visitor control will restrict and control visitor access at all times to rooms, work areas/spaces, and facilities that contain HHS or IHS IT resources. . . .
>
> - A visitor log of all escorted persons entering controlled areas must be maintained at all times. The log will contain the following information.
>
>   - Name of visitor,
>
>   - Purpose of visit,
>
>   - Date and length of visit (time in/time out), and

- Name and position of the authorized person that accompanied the visitor.

Also, *Standard Operating Procedure for General User Security Handbook*, DIS-SOP-06-11a, version 2.4, 10.1.4, "Storage Containers" (page 41) states that "IHS personnel, including contractor support staff, are responsible for providing protection and accountability at all times for all IHS-sensitive information in their control."

IHS Division of Information Security, *Standard Operating Procedure IHS Vulnerability Scanning*, DIS-SOP-16-09, version 1.1, 7.4, "Information Systems Security Officers" (page 12) states that "ISSOs are responsible for supporting network vulnerability scanning and providing guidance to their Area and the system owner for mitigating IT/cybersecurity related risks."

IHS Division of Information Security, *Standard Operating Procedure for Wireless Network Security Standards,* DIS-SOP-09-36, version 2.2, 2, "Standards for Wireless Network Security" (page 5) states that "Designated personnel, such as the local ISSO, must scan wireless local area networks (WLANs) annually or when major changes are made in order to identify and remove any unauthorized wireless access points. The WLAN's entire coverage area must be scanned."

Page 6 of the same reference requires IHS to "Implement 802.1X access control to reduce the risk of access from unauthorized WLAN devices, and provide authentication using a Federal Information Processing Standards (FIPS)-140-validated and Wi-Fi Protected Access 2 (WPA2)-certified Extensible Authentication Protocol (EAP) to verify authorized WLAN devices and/or users."

Page 7 of that same reference states that "Designated personnel should scan for unauthorized wireless APs [access points] (WAPs) annually or when major changes are made. If a rogue WAP is found, the local ISSO must be notified to investigate."

GUIDANCE FROM THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

According to NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments,* chapter 2.4.1 (page 18), 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" (page 7), 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 800-34, 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 [sic] 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 SP 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies* (page 2) recommends that it is necessary to use upgraded software supported by the software's vendor and to have the recommended security patches installed to address new vulnerabilities. Older unsupported software versions become less secure over time.

According to NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers* (page 2-2), it is important to prevent the execution of unauthorized commands or programs on the host operating system, including ones that the intruder has installed, as this may allow attackers to compromise the security of the server and other hosts on the organization's network.

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 Security Management Act for developing information security standards and guidelines, including minimum requirements for Federal information systems.

According to NIST SP 800-53:

- Page F-18 states that an organization should employ "the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

- Pages F-95 and F-96 state that the organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use, and changing default content of authenticators prior to information system installation. Additionally, passwords should have a minimum password complexity, defined by an organization.

- Page F-201 states that information systems should protect the authenticity of communications sessions. "Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions."

- Pages F95-F99 and F-128-F130 state that the organization's implementation policies and procedures requiring individuals to secure physical access devices and to protect authenticator content from unauthorized disclosure and modification. When an individual attempts to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of an individual's identity is needed to make sound access control decisions.

- Page F-151 states that the organization:

    a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

        1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:

1. Risk assessment policy [*Assignment: organization-defined frequency*]; and

2. Risk assessment procedures [*Assignment: organization-defined frequency*].

- Pages F-127 and F-128 state that ... 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.

- Page F-182 states that: "The organization: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs."

- Page F-153 states that organizations are required 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).

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.

APPENDIX E: IHS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES — Public Health Service

MAY 31 2019 — Indian Health Service, Rockville, MD 20857

TO: Inspector General

FROM: Principal Deputy Director

SUBJECT: IHS Comments on OIG Draft Audit Report: *IHS Needs To Improve Oversight of Its Hospitals' Opioid Prescribing and Dispensing Practices and Consider Centralizing Its Information Technology Functions* (A-18-17-11400)

We appreciate the opportunity to review the draft Office of Inspector General (OIG) audit report entitled, "*IHS Needs to Improve Oversight of Its Hospitals' Opioid Prescribing and Dispensing Practices and Consider Centralizing Its Information Technology Functions* (A-18-17-11400)," dated March 21, 2019. The IHS concurs with all of the OIG recommendations. Below you will find a description of the status of actions taken to date to implement the OIG recommendations, and those planned in the near future.

OIG Recommendation No. 1: The IHS concurs with this recommendation.

Revise the Indian Health Manual (IHM) to:

- *Include the type of action a provider should take and what documentation to include in the patient's electronic Health Record (EHR) when a Urine Drug Screen (UDS) is unfavorable.*
- *Require area offices to submit completed annual reviews to IHS Headquarters.*

Actions taken and planned actions as of May 31, 2019

In January 2019, the IHS established a mandatory Headquarters reporting mechanism for required annual audits. All facilities are required to submit annual audits to IHS Headquarters by December 31 of each year, beginning in 2019. By December 31, 2019, the IHS Principal Deputy Director will issue a revision to the IHM that will clearly communicate the type of action a provider should take and specify the documentation to include in the patient's EHR when a UDS is unfavorable.

OIG Recommendation No. 2: The IHS concurs with this recommendation.

Increase oversight of IT systems by IHS management, including consideration of centralizing its key IT systems (including RPMS) services and cybersecurity functions (e.g., patch management, unsupported network equipment, and contingency planning) by conducting a cost-benefit analysis and risk assessment of adopting the Cloud First Policy and other means of

centralization (e.g., Headquarters, IHS Area offices). Specifically, determine if cloud solutions or other modernization approaches are most effective and cost efficient in addressing persistent cybersecurity vulnerabilities and increasing network resiliency.

Actions taken and planned actions as of May 31, 2019

The IHS will coordinate resources to accomplish this recommendation with the support of IHS Area and Service Unit staff. This will include resources to replace necessary infrastructure and establishing controls to ensure compliance is maintained. The IHS Fiscal Year (FY) 2021 budget request will include a justification for additional resources to ensure successful coordination and oversight of all information technology (IT) infrastructure in the IHS. The IHS Office of Information Technology (OIT) will request the use of emergency accreditation funds and nonrecurring expensed funds (NEF) to support initial costs associated with centralization of IT services.

OIG Recommendation No. 3: The IHS concurs with this recommendation.

Present findings and cost savings analysis to Tribal leadership and the IHS user community to get buy-in for any significant IT enterprise changes.

Actions taken and planned actions as of May 31, 2019

Indian Health Manual, Part 3, Chapter 3, "*Capital Planning and Investment Control*," and IHM Part 8, Chapter 4, "*Conducting Information Technology Alternatives Analysis*," requires reviews and analysis of alternatives (including cost-benefit analysis) for IT projects with varying degrees of rigor, depending on the dollar threshold. The IHS intends to revise both chapters to incorporate guidance such as the Modernizing Government Technology Act of 2017 (MGT) and the Federal Information Technology Acquisition Reform Act (FITARA). The IHS is also including a requirement for presentation of findings and cost savings analysis of IT projects with Tribal leadership and with the user community through the IHS Information Systems Advisory Committee (ISAC) and the IHS Chief Information Officers Council (CIOC). The IHS is in the process of formalizing the CIOC with an official charter. The IHS will continue to present to the ISAC and the CIOC, the cost savings associated with contract savings. Beginning in October 2019, the IHS OIT will report on managed services to the ISAC and the CIOC.

OIG Recommendation No. 4: The IHS concurs with this recommendation.

Implement a strategic and phased approach to centralization of IT systems, services, and cybersecurity functions.

Actions taken and planned actions as of May 31, 2019

The Office of the Chief Technology Officer in the Immediate Office of the Secretary, U.S. Department of Health and Human Services (HHS) sponsored the HHS Health Information Technology (HIT) Modernization Research Project for the IHS. This effort will culminate in guidance and recommendations to support a significant budget request necessary to modernize the IHS HIT infrastructure, which includes the IHS Resource and Patient Management System (RPMS). (See also response to recommendation No. 2 above.) The HIT Modernization Research Project started in September 2018 and will conclude in 2019. The IHS plans a 7- to 10-year implementation, with initial budget requests as high as $3 billion dollars. The IHS FY 2020 budget request includes $25 million dollars to support the necessary planning to continue the project and make a final decision on the RPMS replacement. A key component of the modernization is to address the consolidation necessary to centralize management of the EHR environment.

The IHS will develop the plan to centralize IT systems, services, and cybersecurity functions through consultation with IHS leadership, the proposed IHS CIOC, and the ISAC by December 31, 2019. The plan will encompass activities to increase oversight in recommendation No. 2 above and provide the framework to address funding, staffing, and contracts to centralize IT services across the enterprise environment.

OIG Recommendation No. 5: The IHS concurs with this recommendation.

Ensure pain management and related documentation is done in accordance with IHS policies and procedures.

Actions taken and planned actions as of May 31, 2019

The IHS has designed and is currently testing a chronic opioid therapy visit documentation template to assist prescribers with clinical documentation that includes documentation of patient screening results, including SDS and Prescription Drug Monitoring Program (PDMP) checks. It will also assist with documentation of patient treatment plan review. These IT updates will improve compliance by facilities to ensure that pain management and related documentation is accomplished in accordance with IHS policies and procedures.

OIG Recommendation No. 6: The IHS concurs with this recommendation.

Develop policies and procedures to review the EHRs of patients with opioid prescriptions from non-IHS providers and document the results of the review in the EHR, particularly for those patients who had previously violated their COT agreements.

Actions taken and planned actions as of May 31, 2019

By December 31, 2019, the IHS Principal Deputy Director will issue a revision to the IHM that will reinforce to all IHS Areas and Service Units, the requirement to review the EHRs of patients with opioid prescriptions from non-IHS providers and document the results of the review in the EHR, particularly for those patients who had previously violated their Chronic Opioid Treatment (COT) agreements.

OIG Recommendation No. 7: The IHS concurs with this recommendation.

Ensure opioid dispensing data are complete, accurate, and submitted in a timely manner to the State PDMP for use by providers and pharmacists.

Actions taken and planned actions as of May 31, 2019

The IHS has created software programming to automate reporting of controlled substance prescribing data to State-based PDMPs within the required timeframe. This software will ensure that opioid dispensing data are complete, accurate, and submitted in a timely manner to the State PDMP for use by providers and pharmacists. The IHS will complete beta testing by July 31, 2019, with IHS-wide implementation by June 30, 2020.

OIG Recommendation No. 8: The IHS concurs with this recommendation.

Ensure all opioids are in a locked cabinet, safe, drawer, or other appropriate secure container at all times.

Actions taken and planned actions as of May 31, 2019

In October 2018, the IHS revised the IHM, Part 3, Chapter 7, to: 1) include a requirement to lock prescriptions awaiting pick-up; and 2) include a requirement for the Area Pharmacy Consultants to review this requirement for compliance during their annual audits.

OIG Recommendation No. 9: The IHS concurs with this recommendation.

Track all opioids prescribed at the hospital in the patient EHRs, including those being filled at an outside pharmacy.

Actions taken and planned actions as of May 31, 2019

By December 31, 2019, the IHS Principal Deputy Director will issue a directive that IHS prescribers will track in the EHR, all opioids prescribed at IHS facilities, including those being filled at a non-IHS pharmacy.

OIG Recommendation No. 10: The IHS concurs with this recommendation.

Analyze opioid data to make decisions and oversee providers to minimize prescribing practices that exceed daily Milligram Morphine Equivalents (MME) guidelines established by IHS, co-prescribe opioids and benzodiazepines, and use opioids for acute pain

Actions taken and planned actions as of May 31, 2019

In January 2019, the IHS implemented the IHS Safe Opioid Monitoring tool. This facility-level report is submitted monthly to facility and IHS Area leadership. IHS Headquarters is currently tracking the submission of this data. For the first quarter of calendar year 2019, all facilities were 100 percent compliant with submission of their reports.

The report includes the following data:

a. Percent of opioid prescriptions;
b. MME data (including prescriptions with MME ≥ 50 and ≥ 90); and
c. Co-prescribing of opioids with benzodiazepines.

By November 30, 2019, the IHS Heroin, Opioids, and Pain Efforts Committee will complete the development of an opioid stewardship quality assurance program that includes evaluation of opioid-related data on national, regional, and local levels. The data will be used to evaluate population outcomes, target opioid interventions, enhance clinical decision support, and create professional practice evaluation strategies.

OIG Recommendation No. 11: The IHS concurs with this recommendation.

Remediate the IT vulnerabilities identified

Actions taken and planned actions as of May 31, 2019

The IHS details ongoing improvements underway in our response to the supplemental portion of this draft OIG audit report. IHS Headquarters is increasing centralized oversight and monitoring of IT system deficiencies identified in local reviews and related remediation plans. In addition, national policies and procedures addressing the need for standardization and increased oversight by IHS Headquarters are undergoing review and updates. Examples of several key policies under development are described below.

The IHS is currently developing a set of IHM policies related to improved management controls in the IT functional area, which are scheduled to be issued by September 30, 2019. Topics include the IHS CIOC Charter, which will be responsible for coordination of IT systems, services, and cybersecurity in all IHS facilities. The IHS CIOC will meet prior to September 30, 2019, and establish a recurring meeting schedule to ensure operational oversight, incorporate cost saving

analysis for effective IT enterprise management, and address program deficiencies. Additional policies currently under development include IHM, Part 10, Chapter 1, "Cybersecurity Roles and Responsibilities," and IHM, Part 10, Chapter 4, "Audit and Accountability," which will incorporate National Institute of Standards and Technology regulations and guidance. IHM, Part 10, Chapter 14, "Program Management," and IHM, Part 10, Chapter 16, "Risk Assessment," are all estimated to be issued in final by December 31, 2019.

OIG Recommendation No. 12: The IHS concurs with this recommendation.

Renegotiate the Memorandum of Understanding (MOU) with Oklahoma and other states that have restrictive MOU language to allow for PDMP self-audits and collection by clinical directors.

Actions taken and planned actions as of May 31, 2019

The IHS will work to update language in MOUs with all states that allow PDMP self-audits and collection by clinical directors. The IHS will complete amendments to the MOU language and Area Pharmacy Consultants will enter negotiations with the states by July 31, 2019. The IHS projects the completion of new MOUs by December 31, 2020, acknowledging that this timeline will be dependent on cooperation and willingness by states to participate in negotiations.

OIG Recommendation No. 13: The IHS concurs with this recommendation.

Complete required annual reviews that are consistent in type and level of detail across all IHS hospitals.

Actions taken and planned actions as of May 31, 2019

On December 12, 2018, the IHS National Pharmacy Council issued guidance for Area Pharmacy Consultants to implement three standardized annual Area Pharmacy Consultant review tools that are consistent in type and level of detail across all IHS pharmacies. Initial reporting to IHS Headquarters is required for all facilities by December 31, 2019. Additionally, by December 31, 2019, the IHS Principal Deputy Director will issue a directive in the IHM to ensure that this requirement is clearly communicated to all IHS Areas and Service Units.

We sincerely appreciate the opportunity to comment on this draft report. The OIG's feedback will be used to help the IHS improve the Agency's overall management control systems. If you have technical questions about this response, please contact Mr. Darrell LaRoche, Director, Office of Clinical and Preventive Services, IHS, by telephone at (301) 443-4754. Please contact Ms. Athena Elliott, Director, Office of Management Services, IHS, by telephone at (301) 443-5104 with general questions or concerns about the response.

for RADM Michael D. Weahkee, MBA, MHSA
Assistant Surgeon General, U.S. Public Health Service