Department of Health and Human Services

OFFICE OF
INSPECTOR GENERAL

NATIONAL INSTITUTES OF HEALTH HAD INFORMATION TECHNOLOGY CONTROL WEAKNESSES SURROUNDING ITS ELECTRONIC HEALTH RECORD SYSTEM

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

Amy J. Frontz
Deputy Inspector General
for Audit Services

February 2020
A-18-19-06003

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.

National Institutes of Health Had Information Technology Control Weaknesses Surrounding Its Electronic Health Record System

Fiscal Year 2019

Final Report

CLA (CliftonLarsonAllen LLP)
901 North Glebe Road, Suite 200
Arlington, VA 22203-1853
571-227-9500 | fax 571-227-9552
CLAconnect.com

February 17, 2020

Ms. Tamara Lilly
Assistant Inspector General
Office of Audit Services/Cybersecurity & IT Audit Division
330 Independence Avenue, SW
Washington, D.C. 20201

Dear Ms. Lilly:

CliftonLarsonAllen (CLA) LLP is pleased to present our report on the U.S. Department of Health and Human Services (HHS) – National Institutes of Health's (NIH) compliance with information technology controls within its Electronic Health Records (EHR) System.

We appreciate the assistance we received from the Office of Inspector General (OIG) at HHS and the Clinical Center at NIH and appreciate the opportunity to serve you. We will be pleased to discuss any questions you may have.

Very truly yours,

S. M Mirzakhani

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Ms. Tamara Lilly
Assistant Inspector General

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the National Institutes of Health (NIH) compliance with information technology controls within its Electronic Health Records (EHR) System. The objective of the audit was to determine the effectiveness of select NIH Information Technology (IT) controls and how NIH receives, processes, stores and transmits Electronic Health Records (EHR) within its Clinical Research Information System (CRIS).

For this audit, we reviewed select management, technical, and operational controls from the National Institutes of Standards and Technology's (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* over the CRIS system. Specifically, we assessed controls related to access controls, contingency planning, maintenance, risk assessment, system and communication protection, and system and information integrity. Audit fieldwork was performed at NIH's headquarters in Bethesda, Maryland, from March 5, 2019 to July 16, 2019.

Our audit was performed in accordance with *Generally Accepted Government Auditing Standards (GAGAS)*, also known as the Yellow Book, which is issued by the Government Accountability Office (GAO). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We concluded that NIH generally implemented certain security controls for the EHR systems. However, NIH's implementation of certain IT requirements was not fully achieved for a select subset of controls. For example, we noted weaknesses in access controls, contingency planning, and maintenance. As a result, we made three recommendations about how NIH may strengthen IT controls for its EHR system.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. We concluded our fieldwork and assessment on July 16, 2019. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to July 16, 2019.

The purpose of this audit report is to report on our assessment of NIH's compliance with IT controls within its EHR system and is not suitable for any other purpose. Additional information on our findings and recommendations are included in the accompanying report.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
February 17, 2020

Report in Brief
Date: February 2020
Report No. A-18-19-06003

U.S. Department of Health & Human Services
Office of Inspector General

Why We Did This Review

For fiscal year 2019, the Department of Health and Human Services (HHS), Office of Inspector General (OIG) received $5 million in congressional appropriations to conduct oversight of the National Institutes of Health (NIH) grant programs and operations. Among the issues of interest to Congress were matters pertaining to cybersecurity protections and NIH compliance with Federal requirements.

The Clinical Research Information System (CRIS) contains the Electronic Health Records (EHR) for patients of NIH's Clinical Center. The data and the IT security controls protecting the data are of significant importance to both HHS and the Federal government. OIG engaged CliftonLarsonAllen LLP (CLA) to conduct this audit.

The objective was to determine if the EHR System at NIH – also known as CRIS - has effective IT controls and to understand how NIH receives, processes, stores and transmits EHR records into CRIS.

How We Did This Review

To accomplish our objective, CLA reviewed NIH's policies and procedures; tested system security controls and configurations; and inspected public information on NIH's website. CLA also conducted interviews with NIH Clinical Center staff to determine how NIH ensures the integrity of EHR data as well as to document how NIH ingest EHR records.

National Institutes of Health Had Information Technology Control Weaknesses Surrounding Its Electronic Health Record System

What We Found

CLA found that NIH had certain controls in place to secure EHR information and information systems. However, NIH's information security policies and practices were not operating effectively to preserve the security, confidentiality, integrity, and availability of NIH's EHR information and information systems, resulting in potential risks of unauthorized access, use, disclosure, disruption, modification, or destruction. Specifically, (i) the primary and alternate processing sites were located adjacent to each other on the NIH campus and not geographically distinct; (ii) servers supporting the EHR were still in operation despite nearing end-of-life on extended support without an effective transition plan; and (iii) terminated users and inactive accounts were not deactivated in a timely manner.

These weaknesses existed because, at the time of the fieldwork, NIH located their alternate processing site in the same geographic location as their primary site; NIH delayed software upgrades until completion of system upgrades had been completed; and NIH had not yet fully implemented the automated tool that was intended to ensure users and inactive accounts were deactivated timely. CLA shared the preliminary findings with NIH in advance of issuing the draft report. Before issuing the draft report, NIH implemented some of the recommendations.

What We Recommend and NIH Comments

CLA recommends that NIH Clinical Center Management (1) Complete the NIST requirements for implementing an alternative processing site that is a reasonable and viable option. Identify, document, and implement actions to mitigate risks of using existing alternative site based on the risk assessment results until compliant alternate site is established; (2) implement policies and procedures to ensure all software is upgraded or replaced prior to end of life; and (3) ensure that the automated CRIS User Account Management tool is operating so that all changes to user privileges are authorized, properly documented, and inactive accounts are deactivated.

In written comments to the draft report, NIH concurred with all of the recommendations and described actions it has taken or plans to take to address the findings.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181906003.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

For fiscal year (FY) 2019, the Department of Health and Human Services (HHS), Office of Inspector General (OIG) received $5 million in congressional appropriations to conduct oversight of the National Institutes of Health (NIH) grant programs and operations (P.L. No. 115-245).[1] Among the issues of interest to Congress were matters pertaining to cybersecurity protections and NIH compliance with Federal requirements.

The Office of Inspector General at HHS has identified protecting HHS data, systems, and beneficiaries from cybersecurity threats[2] as one of HHS' top management challenges. The Clinical Research Information System (CRIS) contains all Electronic Health Records (EHRs) for patients of the NIH's Clinical Center (the "Clinical Center). In 2018, the Clinical Center had:

- More than 9,700 new patients;
- More than 4,500 inpatient admissions;
- More than 95,000 outpatient visits;
- An average hospital stay of 8.9 days;
- About 1,300 credentialed physicians, dentists, and PhD researchers;
- About 830 nurses;
- About 730 allied health-care professionals, such as pharmacists, dietitians, medical technologists, imaging technologists, therapists, medical records and medical supply staff;
- More than 1,600 laboratories conducting basic and clinical research.[3]

Given the number of patients who receive services at the Clinical Center and the various staff who may have access to their EHRs, the IT security controls play a significant role in protecting access to EHRs.

OBJECTIVE

The objective of this audit was to determine if the EHR System at NIH – referred to also as CRIS – has effective IT controls and to understand how NIH receives, processes, stores and transmits EHR records into CRIS.

BACKGROUND

Management's Responsibility for Assessing Risk and Establishing Internal Controls

Office of Management and Budget (OMB) Circular No. A-123 (the "Circular") requires Federal leaders and managers to integrate enterprise risk management (ERM) in management practices

[1] Department of Defense and Labor, Health and Human Services, and Education Appropriations Act, 2019, and Continuing Appropriations Act, 2019, P.L. No. 115-245, 132 Stat. 2981 (September 28, 2018).

[2] HHS Top Management & Performance Challenges Facing HHS, https://www.oig.hhs.gov/reports-and-publications/top-challenges/2018/

[3] https://clinicalcenter.nih.gov/about/welcome/fact.html

and to establish requirements to assess, correct and report on the effectiveness of internal controls. ERM and internal controls are components of a governance framework. ERM deals with identifying, assessing and managing risks; through adequate risk management, agencies can concentrate efforts toward reducing or eliminating the potential for disruptive events. Internal controls provide a reasonable assurance that the objectives of an entity will be achieved.

The principles underlying this policy are described as follows:

> *Each Federal employee is responsible for safeguarding Federal assets and the efficient delivery of services to the public. Federal leaders and managers are responsible for establishing goals and objectives around operating environments, ensuring compliance with relevant laws and regulations, and managing both expected and unexpected or unanticipated events. They are responsible for implementing management practices that identify, assess, respond, and report on risks. Risk management practices must be forward-looking and designed to help leaders make better decisions, alleviate threats and to identify previously unknown opportunities to improve the efficiency and effectiveness of government operations. Management is also responsible for establishing and maintaining internal controls to achieve specific internal control objectives related to operations, reporting, and compliance.*

The Circular also establishes an assessment framework[4] to properly assess and improve internal controls over operations, reporting and compliance.[5]

The Electronic Health Records System at NIH's Clinical Center

NIH is the primary federal agency responsible for supporting medical research to enhance health, lengthen life, and reduce illness and disability. It has awarded over $30 billion for various types of medical research[6] and has a hospital dedicated to clinical research: the NIH Clinical Center (the "Clinical Center"). The Clinical Center has played a pivotal role in contributing to the development of new therapies, including chemotherapy, tests to detect hepatitis viruses in blood, the first gene therapy, the first treatment for AIDS (with AZT) and the first use of an immunotoxin to treat a malignancy (hairy cell leukemia).[7] As part of the NIH's mission, certain Institutes and Centers provide direct care to patients serving around 10,000 patients per year.[8]

Since opening its doors in 1953, the Clinical Center has expanded to include the Ambulatory Care Research Facility in 1982 and the Mark O. Hatfield Clinical Research Center in 2004. As a result of this expansion, approximately 1,840 employees and 1,300 credentialed and privileged

[4] The framework is based on the Government Accountability Office (GAO)'s *Standards for Internal Control in the Federal Government* (The Green Book).

[5] *Management's Responsibility for Enterprise Risk Management and Internal Control*, issued July 15, 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[6] https://www.nih.gov/grants-funding

[7] https://clinicalcenter.nih.gov/about/welcome/faq.html

[8] https://clinicalcenter.nih.gov/ccc/crc/

physicians support 1,600 ongoing clinical research studies.[9] To assist in managing patient care, NIH utilizes a commercial, off-the-shelf EHR product by Allscripts®, called Sunrise Acute Care Manager, which is the primary operating software for CRIS.

HOW WE CONDUCTED THIS AUDIT

For this audit, CLA reviewed whether certain management, technical, and operational controls[10] were in place for CRIS*.* Specifically, CLA reviewed the following:

- access controls;
- contingency planning;
- maintenance;
- risk assessment;
- system and communication protection; and
- system and information integrity.

Audit fieldwork was performed at NIH's headquarters in Bethesda, Maryland, from March 5, 2019 to July 16, 2019.

The audit was performed in accordance with *Generally Accepted Government Auditing Standards (GAGAS)*, also known as the Yellow Book, which is issued by Government Accountability Office (GAO). 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 the findings and conclusions.

To accomplish the audit objectives, CLA reviewed applicable federal laws, regulations and guidance; interviewed NIH's Department of Clinical Research Informatics (DCRI) - Clinical Center & Health Information Management Department (HIMD) personnel; evaluated NIH's policies, procedures, standard operating procedures, manuals, guides, and practices for EHR processing, transmission, storage and disposal. CLA also reviewed information available on NIH's publicly accessible website. CLA communicated to NIH the preliminary findings in advance of issuing the draft report.

Appendix A describes the audit scope and methodology.

FINDINGS

CLA found that NIH had certain controls in place to secure EHR information and information systems. However, NIH's information security policies and practices were not operating effectively to preserve the security, confidentiality, integrity, and availability of NIH's EHR information and information systems, resulting in potential risks of unauthorized access, use, disclosure, disruption, modification, or destruction. Specifically:

1. NIH did not ensure that the alternate processing site for its EHR system was sufficiently

[9] U.S. Department of Health and Human Services. "About NIH" et seq. *National Institutes of Health,* 2019, https://www.nih.gov/about-nih

[10] The controls were selected from the National Institutes of Standards and Technology's (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

separated from the primary processing site.
2. NIH did not upgrade all servers supporting the EHR information system in a timely manner.
3. NIH account management processes were not operating effectively.

These weaknesses existed because (i) NIH located their alternate processing site in the same geographic location as their primary site; (ii) NIH delayed software upgrades until completion of system upgrades had been completed; and (iii) NIH had not yet fully implemented the automated tool that was intended to ensure users and inactive accounts were deactivated timely.

After CLA concluded the audit, but before we issued the report, NIH provided CLA with evidence indicating that it had implemented some of the recommendations. CLA continues to report the findings as identified and included a brief description of the actions NIH has taken to address the findings.

EHR ALTERNATE PROCESSING SITE WAS NOT SUFFICIENTLY SEPARATED FROM PRIMARY PROCESSING SITE

The alternate processing site for CRIS is in a building next to its primary processing site on the NIH campus. The two are not in geographically distinct locations as required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series were developed in accordance with the statutory responsibilities of NIST under the Federal Information Security Modernization Act (FISMA) of 2014.[11] The SP 800 publications are intended to address and support the security and privacy needs of U.S. Federal Government information and information systems.[12]

As provided in NIST SP 800-34, Revision 1, organizations must have a process in place to minimize the risk of unintended interruptions and to recover critical operations when prolonged interruptions occur. Alternate processing sites provide a location for an organization to resume system operations when a catastrophic event disables or destroys the system's primary processing site.[13] Alternate processing sites must be sufficiently separated (i.e., located in a geographically distinct area from primary processing sites) from primary processing sites and are intended to provide processing capability in the event that the primary processing site is not available.

If an agency has an alternative processing site that is subject to the same event(s) as its primary site, a risk assessment is required.[14] Risk assessments consider threats and vulnerabilities to identify and evaluate risk in terms of likelihood of occurrence and potential adverse impact (e.g., magnitude of harm) to organizations, assets, and individuals. Risk assessments may take into account a variety of factors, including geographic area, accessibility of the site, security, environment, and cost of offsite storage. Other factors typically considered are the risks of natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission.

[11] 44 U.S.C. § 3551 *et. seq.*, Public Law (P.L.) 113-283.

[12] https://www.nist.gov/itl/nist-special-publication-800-series-general-information

[13] NIST Special Publication 800-34, Revision 1.

[14] NIST Special Publication 800-53, Revision 4.

NIH cited budgetary constraints as one of several reasons why it has not been able to secure funding for a NIST-compliant alternate processing site. NIH Management also indicated that they had taken steps to mitigate the risk of not having an alternate processing site sufficiently separated from the primary processing site. For example, NIH has procured servers to restore data from backup tapes stored at a local third-party vendor.

In a January 2018 *Alternate Processing Site Risk Waiver–ID # 10897,*[15] NIH acknowledged that, "In the event of natural disasters, structural failures or hostile cyber-attacks against the NIH enterprise network, both data centers would be susceptible to the same threats due to the co-location on the main NIH campus with the same network backbone." Accordingly, the effectiveness of NIH's disaster recovery strategy likely would be handicapped by (i) substantial delays associated with restoring data from backups stored off-site; (ii) the necessity to procure and install physical server hardware to access data; and (iii) the paucity of available human capital resources to re-establish network connectivity.

During the course of the audit, the Clinical Center stated that it had identified a new alternate processing site for CRIS. However, CLA found this location also was not sufficiently separated from the primary processing site and was susceptible to the same hazards identified at the primary processing site. Additionally, NIH had not conducted a NIST-compliant risk assessment for the new location that, "identifies, prioritizes, and estimates risk to organizational operations (i.e., mission, functions, image, reputation, etc.), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems. NIH officials did not provide an *Alternate Processing Site Risk Waiver* for the new location.

These inadequacies existed because NIH had not - as required by NIST – situated the alternate site in a location geographically distinct from the primary site and had not assessed the risk that the new alternate processing site would be susceptible to the same threats as the primary processing site. As a result, the hospital may not have an alternative means to access EHR data because one threat could halt processing at both sites. This would not only adversely affect patient care, but also present profound implications for patient harm.

SERVERS SUPPORTING THE EHR INFORMATION SYSTEM NOT UPGRADED TIMELY

Information system components present increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. To address the risk that components may not be functional or may become dysfunctional, organizations enter into preventative maintenance contracts.

Preventive maintenance includes taking proactive steps to service organizational information systems components for the purpose of maintaining equipment and facilities in satisfactory operating condition. Such maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects.[16]

[15] An Alternate Process Site Risk Waiver is typically completed when an organization has accepted certain key risks associated with the alternate processing site.

[16] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The audit identified four CRIS servers running an operating system for which Microsoft Corporation stopped providing mainstream software support[17] in 2015. Extended support from Microsoft Corporation runs through January 2020, which provides NIH with access to software updates.

This weakness existed because NIH was in the process of upgrading its hardware in anticipation of upgrading CRIS, which would be accompanied by a software upgrade. However, NIH had not completed this exercise at the time of the audit. According to NIH, the current operating system will not support the upgraded version of CRIS.

Industry standards show that systems nearing end of life on extended support may be susceptible to older vulnerabilities and exploitation. Among other reasons, vendors release upgraded versions of products to address weaknesses identified and limit or eliminate support of older versions which then remain susceptible to the known vulnerability. This may potentially expose NIH resources, including CRIS, to unauthorized use by malicious actors who may take advantage of vulnerabilities with the operating system in use.

After CLA concluded the fieldwork, but before we issued the report, NIH provided documents indicating that it had remedied server vulnerabilities by upgrading four servers to vendor-supported versions. Per the executed contract with the vendor, these servers are also nearing end-of-life but will have mainstream support through 2023.

ACCOUNT MANAGEMENT PROCESSES WERE NOT OPERATING EFFECTIVELY

Account management controls limit inappropriate access to information systems and protect the agency's data from unauthorized modification, loss and disclosure. For account management controls to be effective, they must be consistently implemented and monitored.

Organizations determine which account management controls are appropriate for different types of employment actions, whether permanent or temporary. For example, actions that may be required for personnel transfers or reassignments within organizations include: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (e.g., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.

CLA found that the Clinical Center did not perform effective account management controls for CRIS. Specifically, CLA noted:

- From 26 user accounts that were inactive for a period greater than 365 days, 19 user accounts remained active without being deactivated.
- From 61 terminated users with access to CRIS, 9 terminated users still had active accounts in the system.
- 3 out of 25 sampled new CRIS users had changes to their account privileges without a form justifying and documenting these changes.

[17] Mainstream Support includes: Incident support (no-charge incident support, paid incident support, support charged on an hourly basis, support for warranty claims); Security update support.

According to the *NIH Information Security Handbook*, user accounts that are inactive for more than 365 days must be deactivated.[18] NIH "…employs automated mechanisms to support the management of information system accounts.…The information system automatically disables inactive accounts after 60 days or less…The information system automatically disables temporary accounts after 180 days or less while emergency accounts should be removed after 60 days or less."[19]

These weaknesses existed because the recently implemented automated CRIS User Account Management tool to identify inactive accounts and any employees who were terminated or transferred between NIH's Institutes or Centers is not operating as designed. The new tool was intended to replace the manually intensive process of account management. For example, the automated tool does not properly track an employee's transfer between departments at NIH, which may inform whether system access should be revoked or deactivated. NIH management continues to work on improving the tool.

If system access is not revoked or deactivated in a timely manner for persons who no longer require access, NIH's EHR data and resources may be exposed to unauthorized access and misuse. In addition, inactive accounts that are not disabled when employees separate from NIH may be used to gain access to NIH data and sensitive information. Moreover, unauthorized changes to user access levels may give users access to resources they do not need or require in the daily execution of their duties, further risking EHR data to unauthorized use.

RECOMMENDATIONS

CLA recommends that Clinical Center management implement the specific recommendations below to enhance its information security environment related to its EHR systems. CLA recommends that the Clinical Center:

1. Complete the NIST requirements for implementing an alternative processing site that is a reasonable and viable option. Identify, document, and implement actions to mitigate risks of using existing alternative site based on the risk assessment results until compliant alternate site is established.
2. Implement policies and procedures to ensure all software is upgraded or replaced prior to end of life.
3. Ensure that the automated CRIS User Account Management tool is operating as intended and confirm that all changes to user privileges are authorized, properly documented, and inactive accounts are deactivated.

OTHER MATTERS

CLA's review of how NIH receives, processes, stores and transmits EHR records encompassed a combination of: inquiry with Clinical Center and Health Information Management Department personnel, observation of the Electronic Health Record Management presentation and inspection of a variety of artifacts. Interface strategy and design documentation were reviewed to determine how interconnections are identified, built and secured to ensure data confidentiality, integrity, availability and privacy. Interconnection security agreement (ISA) and memorandum of understanding (MOU) standard operating procedures were inspected to determine how they are

[18] *NIH Information Security Handbook*: Control ID AC-2.

[19] *NIH Information Security Handbook: Control ID AC-2 c.e.1, c.e.2* & c.e.3.

documented, their duration, security provisions and assessment and authorization related requirements. CRIS dataflows were reviewed to determine the sources, nature and security of data flowing into CRIS. CRIS inventory of interconnections was reviewed to verify cataloguing and monitoring of internal connections was taking place.

Outside records received by NIH such as medical records, reports, schedules, calendars or patient/referring clinician letters follow a separate process whereby they are converted to PDF and reviewed by the Health Information Management Department for accuracy before they are uploaded into CRIS. Outside records related to Clinical Center results are converted to PDF and paired with a corresponding order number. The date, result type, and PDF are entered into the patient's EHR and digitally signed prior to submission in CRIS.

NIH COMMENTS AND AUDITOR RESPONSE

In written comments to the draft report, NIH concurred with all of the recommendations. NIH indicated and provided supporting documentation that it had already implemented recommendations (2) and (3) and would continue implementing the remaining recommendation. After reviewing the supporting documentation, we agree that recommendations (2) and (3) have been implemented and recommend the findings be closed.

NIH's comments are included as Appendix B. Management comments referenced an *Appendix to General Comments with Supporting Documents* that are not included in the report due to the sensitivity of the information.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

CLA limited the audit to NIH's policies, processes, and procedures regarding:

- The identification of risks and deficiencies associated with the processes NIH uses to receives, processes, stores and transmits EHR records, system interfaces, and the accuracy and completeness of information. The assessment requirements in the areas of select security controls of NIH's EHR systems.
- Select management, technical, and operational controls from the NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*:
  - Access Controls
  - Contingency Planning
  - Maintenance
  - Risk Assessment
  - System and Communications Protection
  - System and Information Integrity
- Select controls identified in GAOs *Federal Information Systems Control Audit Manual (FISCAM)* related to interface controls.

METHODOLOGY

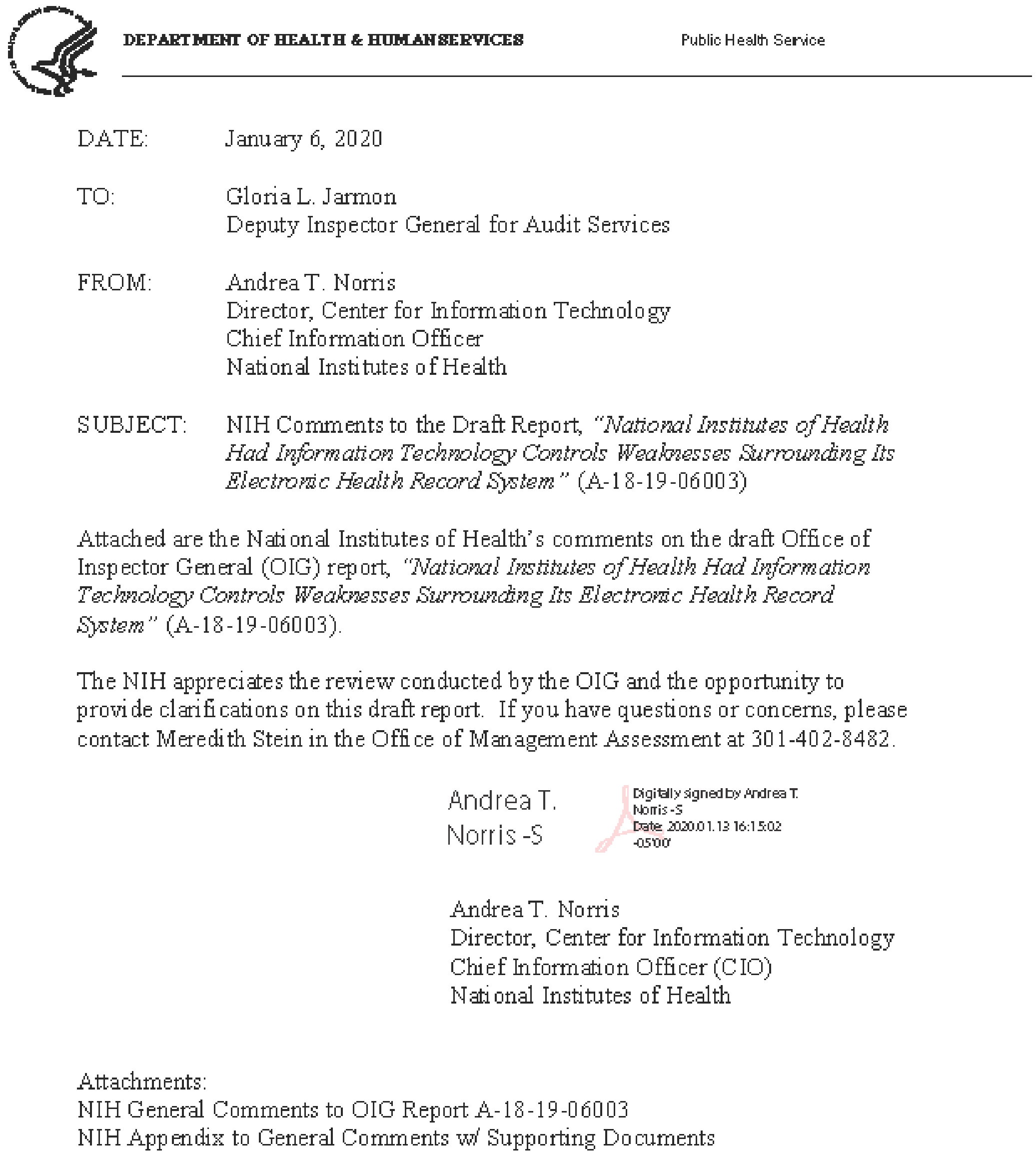
To accomplish the objective, CLA:

- Reviewed applicable federal laws, regulations and guidance.
- Interviewed NIH's Department of Clinical Research Informatics (DCRI) - Clinical Center & Health Information Management Department (HIMD) personnel.
- Assessed NIH's policies, procedures, standard operating procedures, guides, and practices for EHR processing, transmission, storage and disposal.
- Where appropriate, CLA compared documents, such as NIH's information technology policies and procedures, to requirements stipulated in NIST special publications.
- Performed tests of system processes to determine the adequacy and effectiveness of those controls.
- Reviewed public information available on NIH's website.
- Discussed the results of the audit with NIH officials.

In selecting and testing for the adequacy and effectiveness of controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk, and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population. However, in cases where the entire audit population was not selected, the results cannot be projected and if projected may be misleading.

CLA conducted this audit in accordance with performance auditing standards, as in accordance with *Generally Accepted Government Auditing Standards (GAGAS)*, also known as the Yellow Book, which is issued by the Government Accountability Office (GAO). Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objective.

APPENDIX B: NIH COMMENTS



DEPARTMENT OF HEALTH & HUMAN SERVICES Public Health Service

DATE: January 6, 2020

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

FROM: Andrea T. Norris
Director, Center for Information Technology
Chief Information Officer
National Institutes of Health

SUBJECT: NIH Comments to the Draft Report, *"National Institutes of Health Had Information Technology Controls Weaknesses Surrounding Its Electronic Health Record System"* (A-18-19-06003)

Attached are the National Institutes of Health's comments on the draft Office of Inspector General (OIG) report, *"National Institutes of Health Had Information Technology Controls Weaknesses Surrounding Its Electronic Health Record System"* (A-18-19-06003).

The NIH appreciates the review conducted by the OIG and the opportunity to provide clarifications on this draft report. If you have questions or concerns, please contact Meredith Stein in the Office of Management Assessment at 301-402-8482.

Andrea T.
Norris -S

Digitally signed by Andrea T.
Norris -S
Date: 2020.01.13 16:15:02
-05'00'

Andrea T. Norris
Director, Center for Information Technology
Chief Information Officer (CIO)
National Institutes of Health

Attachments:
NIH General Comments to OIG Report A-18-19-06003
NIH Appendix to General Comments w/ Supporting Documents

GENERAL COMMENTS OF THE NATIONAL INSTITUTES OF HEALTH (NIH) ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) OFFICE OF INSPECTOR GENERAL (OIG) DRAFT REPORT ENTITLED: "THE NATIONAL INSTITUTES OF HEALTH HAD INFORMATION TECHNOLOGY CONTROLS WEAKNESSES SURROUNDING ITS ELECTRONIC HEALTH RECORD SYSTEM" (A-18-19-06003)

The National Institutes of Health (NIH) appreciates the review conducted by OIG and the opportunity to provide clarifications on this draft report. NIH respectfully submits the following general comments.

OIG Recommendation 1:

Complete the NIST requirements for implementing an alternative processing site that is a reasonable and viable option. Identify, document, and implement actions to mitigate risks of using existing alternative site based on the risk assessment results until compliant alternate site is established.

NIH Response:

The NIH concurs with OIG's finding and corresponding recommendation.

The NIH will review the requirements for implementing an alternative processing site and identify, document, and implement appropriate actions based on the risk assessment results.

Please reference *Appendix* for additional details on the steps taken.

Target Completion Date: March 31, 2020.

OIG Recommendation 2:

Implement policies and procedures to ensure all software is upgraded or replaced prior to end of life (EOL).

NIH Response:

NIH concurs with OIG's finding and corresponding recommendation.

Since September 2019, NIH Clinical Center (CC) has implemented policies and procedures to ensure that all software is upgraded or replaced prior to EOL. Furthermore, in addition to the policies and procedures recommended, NIH CC has implemented a plan to ensure that software and related system assets are upgraded and replaced prior to EOL.

Please reference *Appendix* for additional details on the steps taken.

Based on these actions as described and evidence referenced in the supporting documentation, NIH requests that this recommendation be closed as implemented.

Completion Date: January 31, 2020.

OIG Recommendation 3:

Ensure that the automated CRIS User Account Management tool is operating as intended and confirm that all changes to user privileges authorized, properly documented, and inactive accounts are deactivated.

<u>NIH Response:</u>
NIH concurs with OIG's finding and corresponding recommendation.

NIH has taken steps to ensure that the automated CRIS User Account Management tool is operating as intended. And, as of December 1, 2019, NIH has confirmed that all changes to user privileges are authorized, properly documented and that inactive accounts are deactivated.

To ensure that the automated tool is operating as intended, the NIH CC has ensured the CRIS User Account Management tool and processes for the tool were updated in June 2019. In addition, the Standard Operating Procedure for the system was updated to reflect the changes to procedures to also include the CRIS User Management tool. This procedure was approved on July 18, 2019.

Additionally, NIH has confirmed that all changes to user privileges are authorized, properly documented and that inactive accounts are deactivated by performing an internal, systematic verification from August - November 2019.

Please reference *Appendix* for additional details on the steps taken.

Based on these actions as described and evidence referenced in the supporting documentation, NIH requests that this recommendation be closed as implemented.

Completion Date: December 1, 2019.