United States Government Accountability Office



Report to Congressional Requesters

January 2018

COAST GUARD HEALTH RECORDS

Timely Acquisition of New System Is Critical to Overcoming Challenges with Paper Process

This Report Is Temporarily Restricted Pending Official Public Release.

GAO-18-59

January 2018

COAST GUARD HEALTH RECORDS

Timely Acquisition of New System Is Critical to Overcoming Challenges with Paper Process

GAO Highlights

Highlights of GAO-18-59, a report to congressional requesters

Why GAO Did This Study

In 2010, the Coast Guard initiated an effort—known as IHiS—to replace its aging EHR system with a suite of modernized systems that was to automate various health care services for its nearly 50,000 military members. However, in October 2015, the Coast Guard announced that the modernization project would be canceled.

GAO was asked to review the Coast Guard's efforts to develop a modernized EHR system. GAO's objectives were to (1) describe what led the Coast Guard to terminate further IHiS development, and how much was spent on the project; (2) evaluate the Coast Guard's management and oversight for the discontinued project and what, if any, lessons learned were identified; (3) describe the Coast Guard's current process for managing health records and the challenges, if any, it is encountering; and (4) determine the Coast Guard's plans for effectively implementing a new EHR system and the current status of its efforts. To do so, GAO reviewed project expenditures, analyzed key project management documentation, surveyed Regional Managers and clinical staff, and interviewed knowledgeable staff.

What GAO Recommends

GAO is recommending the Coast Guard (1) expeditiously and judiciously pursue the acquisition of a new EHR system, and in doing so (2) ensure key processes are implemented, (3) establish project governance boards, and (4) document lessons learned. The Department of Homeland Security concurred with GAO's recommendations.

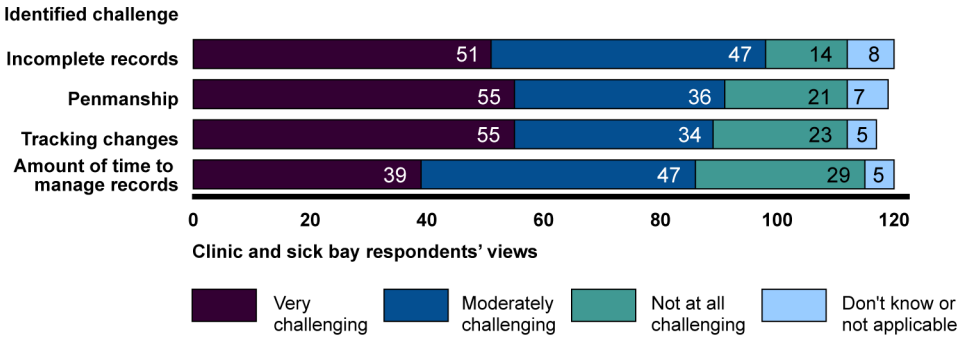
View GAO-18-59. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Financial, technical, schedule, and personnel risks led to the United States Coast Guard's (Coast Guard) decision to terminate the Integrated Health Information System (IHiS) project in 2015. According to the Coast Guard (a military service within the Department of Homeland Security), as of August 2017, $59.9 million was spent on the project over nearly 7 years and no equipment or software could be reused for future efforts. In addition, the Coast Guard could not fully demonstrate the project management actions taken for IHiS, lacked governance mechanisms, and did not document lessons learned for the failed project.

As a result of the cancelation of the IHiS project and the decommissioning of the two legacy electronic health record (EHR) systems IHiS was to replace, the Coast Guard directed its clinics to revert to maintaining health records using a predominantly paper process. Coast Guard Regional Managers and clinic and sick bay administrators informed GAO of the many challenges encountered in returning to a paper process. These challenges include the inability for some clinics to adequately track vital information such as the medications members are taking—potentially causing harm to them.

Top Four Challenges Reported by Clinic and Sick Bay Administrators in Managing Paper Heath Records



Source: GAO survey data. | GAO-18-59

To help alleviate several of these challenges, the Coast Guard has developed alternative work-around processes. However, these alternative processes may not provide sustained solutions to overcoming these challenges.

In February 2016, the Coast Guard initiated the process for acquiring a new EHR system. As of November 2017, agency officials had conducted research and recommended a solution based on performance, risk, cost, and schedule advantages. However, 2 years after canceling IHiS and moving toward a predominately manual process, the agency has not yet made a final determination on this. Successfully and quickly implementing an EHR system is vital to overcoming the challenges Coast Guard currently faces in managing paper health records. The expeditious implementation of such a system can significantly improve the quality and efficiency of care to the thousands of Coast Guard active duty and reserve members that receive health care.

Contents

Letter		1
	Background	4
	The Coast Guard Attributed IHiS Termination to Financial and Other Risks, after Spending Approximately $60 Million on the Project	8
	The Coast Guard Could Not Demonstrate Effective Project Management, Lacked Governance Mechanisms, and Did Not Document Lessons Learned for the IHiS Project	11
	The Coast Guard Is Managing Health Records Using a Predominately Paper Process; Many Challenges Hinder Service Delivery	22
	The Coast Guard Intends to Acquire a New EHR System, but Has Not Yet Chosen a Solution	33
	Conclusions	36
	Recommendations for Executive Action	37
	Agency Comments and Our Evaluation	38
Appendix I	Objectives, Scope, and Methodology	40
Appendix II	Summary of the Coast Guard's SDLC Phases and Selected Project Management Practices	44
Appendix III	Copy of the Survey That GAO Administered to Coast Guard Health Safety and Work-Life Regional Managers	48
Appendix IV	Copy of the Survey That GAO Administered to Coast Guard Clinic and Sick Bay Administrators	52
Appendix V	Summary of the Coast Guard's Non-Major Acquisition Process Acquisition Decision Events and Phases	61

VI Comments from the Department of Homeland Security 62

Appendix VII GAO Contact and Staff Acknowledgments 65

Table

Table 1: Extent to Which the Coast Guard Demonstrated the Completion of Selected Systems Development Life Cycle (SDLC) Project Management Practices 12

Figures

Figure 1: General Steps That the Coast Guard's Clinical Staff Are to Follow to Process Paper Health Records 24
Figure 2: Clinic and Sick Bay Survey Respondents' Views of the Challenges Identified by Regional Managers in Managing and Maintaining Paper Health Records 26
Figure 3: Examples of a Coast Guard Paper Health Record with Multiple Volumes and Storage Cabinets 29
Figure 4: The Coast Guard's Acquisition Decision Events and Phases for Non-Major Acquisition Programs 34

Abbreviations

ADE	Acquisition Decision Event
AHLTA	Armed Forces Health Longitudinal Technology Application
ATO	authority to operate
C4&IT	Command, Control, Communications, Computers, and Information Technology
Coast Guard	United States Coast Guard
COTS	commercial off-the-shelf
CHCS	Composite Health Care System
CIO	Chief Information Officer
DHA	Defense Health Agency
DOD	Department of Defense
EHR	electronic health record
eHRa	Electronic Health Record Acquisition
EOC	Executive Oversight Council
HSWL	Health, Safety and Work-Life
IHiS	Integrated Health Information System
IT	information technology
NMAP	Non-Major Acquisition Process
PGUI	Provider Graphical User Interface
SDLC	System Development Life Cycle
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 24, 2018

The Honorable John Thune
Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Bill Shuster
Chairman
The Honorable Peter A. DeFazio
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Duncan Hunter
Chairman
The Honorable John Garamendi
Ranking Member
Subcommittee on Coast Guard and Maritime Transportation
House of Representatives

The Honorable Dan Sullivan
United States Senate

The United States Coast Guard (Coast Guard), a military service within the Department of Homeland Security, is the principal federal agency responsible for maritime safety, security, and environmental stewardship in U.S. ports and waterways. In addition, the Coast Guard acts as a first responder and provides humanitarian services that aid individuals in distress or those impacted by natural and man-made disasters, whether at sea or ashore. The Coast Guard is also a law enforcement and regulatory agency with broad legal authorities associated with maritime transportation, hazardous materials shipping, bridge administration, oil spill response, pilotage, and vessel construction and operation.

In support of its missions, the Coast Guard is tasked with providing health care to active duty and reserve members; ensuring the medical and dental readiness of all Coast Guard members to maintain their ability for worldwide deployment; and ensuring the availability of quality, cost-effective health care for all eligible beneficiaries. To assist with this task, the Coast Guard has historically relied on electronic health record (EHR)

systems to perform such functions as scheduling patient appointments, documenting patient consults and referrals, and tracking prescribed medications.

In 2010, the Coast Guard initiated an effort to replace its aging EHR systems with a suite of modernized systems called the Integrated Health Information System (IHiS). This system was to modernize various health care services and provide additional functionality, such as a document management system, which was previously lacking. However, in October 2015, the Coast Guard announced that the modernization project would be canceled.

In light of this decision, you asked us to review the Coast Guard's actions related to its EHR modernization initiative and its current health records management process. Our specific objectives were to (1) describe what led the Coast Guard to the decision to terminate further IHiS development, and how much was spent on the project; (2) evaluate the Coast Guard's management and oversight actions for the discontinued EHR modernization project and what, if any, lessons learned were identified; (3) describe the Coast Guard's current process for managing health records and the challenges, if any, it is encountering; and (4) determine the Coast Guard's plans for effectively implementing a new EHR system and the current status of its efforts.

To address the first objective, we reviewed relevant IHiS documentation, such as key contracts, the project plan, presentations by the project management team regarding the status of development efforts, and IHiS-related memorandums. We also reviewed project expenditures documentation developed by the Deputy Commandant for Mission Support and the Acquisition Directorate.[1] We supplemented our review with interviews of agency officials within the Coast Guard's Health Safety and Work-Life (HSWL) Directorate, Office of Budget and Programs, Office of Resource Management, Office of Contract Operations, and Office of Acquisition Support, along with interviews of six key IHiS contractors.

To address the second objective, we reviewed the *Coast Guard's Command, Control, Communications, Computers, and Information*

[1]The Acquisition Directorate, led by the Deputy Assistant Commandant for Acquisition and Chief Acquisition Officer, is responsible for, among other things, planning, directing, coordinating, and controlling all aspects of procurement policy and operational contracting programs; and supporting all aspects of the acquisition enterprise.

Technology (C4&IT)[2] *System Development Life Cycle (SDLC) Policy*[3] *and SDLC Practice Manual*[4] intended to guide the management and oversight of the agency's acquisition projects. We compared available project management documentation, such as project plans, the project's schedule, decision memorandums, and Executive Oversight Council (EOC) meeting minutes, which demonstrated actions taken by project management staff during the IHiS project, against key SDLC Practice Manual requirements. These included fundamental practices for conceptual planning, planning and requirements, design, and development and testing. In addition, we interviewed responsible Coast Guard officials and contractors regarding their role in the project and determined whether officials documented lessons learned for future decisions for the new EHR project.

To address the third objective, we reviewed Coast Guard medical records management documentation, such as medical manuals, workflow procedures, and standard operating policies and procedures for the Coast Guard's 166 clinics and sick bays. We also administered a survey via e-mail to all of the 12 HSWL Regional Managers[5] and a web-based survey to all of the 166 clinic and sick bay administrators to obtain their views on any challenges they face in managing paper health records, as well as any mitigation strategies they have employed for the challenges they identified.

Before administering the surveys, we pretested them by interviewing 1 Regional Manager and 5 clinic and sick bay administrators to ensure survey questions were accurately reflected. We received responses to the survey from all 12 Regional Managers and from 120 of the 166 clinic and sick bay administrators.

[2]C4&IT is responsible for designing, developing, deploying, and maintaining C4&IT solutions for the entire Coast Guard. The Deputy Assistant Commandant for C4&IT serves as the Coast Guard's Chief Information Officer (CIO).

[3]Coast Guard, *Command, Control, Communications, Computers and Information Technology (C4&IT) System Development Life Cycle (SDLC) Policy, Commandant Instruction 5230.66A* (Washington, D.C.: Dec. 11, 2009).

[4]Coast Guard, *U.S. Coast Guard Systems Development Life Cycle (SDLC) Practice Manual, Revision 1.0* (Washington, D.C.: Dec. 11, 2009); and *U.S. Coast Guard SDLC Practice Manual, SDLC Product #107 Revision 4.0* (Washington, D.C.: Nov. 30, 2011).

[5]HSWL Regional Managers provide oversight and supervision of medical administrative functions of all clinics, sickbays, and Work-Life staffs in the HSWL area of responsibility.

To address the fourth objective, we reviewed available planning documentation, such as a request for information,[6] capabilities analysis study plan and report, and the alternatives analysis report for the acquisition or development of a new EHR system as of October 2017. We also interviewed officials within the Acquisition Directorate to determine the status of the efforts to acquire or develop a new EHR system. A full description of our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from October 2016 to January 2018 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.

Background

Electronic health records that are interoperable[7] and contain all relevant patient information are crucial for optimizing the health care provided to patients. Historically, patient health information has been scattered across paper records kept by different caregivers in many different locations, making it difficult for a clinician to access all of a patient's health information at the time of care. Lacking access to these critical data, a clinician may be challenged in making the most informed decisions on treatment options, potentially putting the patient's health at risk. Thus, the move toward collecting, storing, retrieving, and transferring these records electronically can significantly improve the quality and efficiency of care.

This is especially true in the case of military personnel and veterans, such as those in the Coast Guard, because they tend to be highly mobile and may have health records at multiple facilities both within and outside the United States. Therefore, EHRs that are interoperable among health care systems of providers such as the Coast Guard, the Department of

[6]The request for information was part of a market research effort to assess industry capabilities that would best address the Coast Guard's needs for a new EHR system.

[7]According to the Institute of Electrical and Electronics Engineers, interoperability is defined as the ability of a system or a product to work with other systems or products without special effort on the part of the customer. Thus, in this context, interoperability allows patients' electronic health information to be available from provider to provider, regardless of where the information originated.

Defense (DOD), and the Department of Veterans Affairs (VA) are key to improving the care these patients receive.

In April 2004, the President called for widespread adoption of interoperable EHRs by 2014.[8] Similarly, in August 2006, the President instructed agencies, as they implemented, acquired, or upgraded health information technology (IT) systems, to utilize systems and products that met recognized interoperability standards.[9] For nearly two decades both DOD and VA have been working to implement interoperable health care systems, although with little success.[10]

The Coast Guard Has Historically Relied on EHRs and Related Systems to Support Health Care Efforts

The Coast Guard's HSWL Directorate is responsible for ensuring the readiness and health of nearly 50,000 members throughout the United States. In this regard, the Office of Health Services within HSWL is charged with providing healthcare to Coast Guard members, other military active duty and reserve members, retired personnel, and eligible family members. The Coast Guard's healthcare services are supported by 41 U.S. based health clinics and 125 sick bays.[11]

In an effort to meet the need for interoperable EHRs, in 2002, the Coast Guard implemented DOD's Composite Health Care System (CHCS)[12] at its clinics and sickbays. According to the Coast Guard's medical manual, the clinics and sickbays used CHCS for various health care-related activities, including scheduling patient appointments; documenting patient

[8]Executive Order 13335, *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator* (Apr. 27, 2004).

[9]Executive Order 13410, *Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs* (Aug. 22, 2006).

[10]For more information on their efforts, see GAO, *Electronic Health Records: Outcome-Oriented Metrics and Goals Needed to Gauge DOD's and VA's Progress in Achieving Interoperability*, GAO-15-530 (Washington, D.C.: Aug. 13, 2015).

[11]A sick bay is a small medical treatment facility, afloat or ashore, normally staffed only by Health Services Technicians for the care and treatment of active duty personnel.

[12]According to Coast Guard, CHCS was a fully integrated health care information system that connected Coast Guard's medical clinics to computerized patient records that were created and maintained by Coast Guard to provide health care services to its patients. For more information on CHCS, see GAO, *Information Technology: Opportunities Exist to Improve Management of DOD's Electronic Health Record Initiative*, GAO-11-50 (Washington, D.C.: Oct. 16, 2010).

consults and referrals; storing prescriptions; tracking and controlling prescribed medications; and tracking laboratory orders. CHCS interfaced with the DOD Defense Eligibility Enrollment Reporting System, which provided verification of the identity and benefit eligibility of Coast Guard members; other military active duty, reserve, and retired personnel; and their eligible family members. CHCS also interfaced with other health care-related systems, such as a DOD prescription repository, a patient lab delivery system used by health care providers, a system that provided eyewear-related services, and the military's health insurance provider's system.

To provide a more user-friendly way of accessing CHCS, the Coast Guard implemented DOD's Provider Graphical User Interface (PGUI)[13] in 2004. This interface also provided clinics and sick bays with additional system functionality, such as the ability to create and store medical notes electronically.

According to HSWL staff, although CHCS and PGUI provided the Coast Guard with a way to manage health records electronically, these systems were outdated and lacked key functionality such as billing, scheduling, and case management. Therefore, the Coast Guard intended to transition from CHCS and PGUI to DOD's more modernized Armed Forces Health Longitudinal Technology Application (AHLTA) in 2009 to achieve interoperability with DOD and VA and comply with executive orders and statutes that called for efficient health care initiatives. However, HSWL staff stated that the cost of adopting and maintaining AHLTA, as well as the need for the Coast Guard to meet its unique mission requirements, led the agency to move forward with implementing a new system of its own in 2010. The new system was intended to be interoperable with both DOD's and VA's health information systems.

Toward this end, on September 30, 2010, the Coast Guard awarded a 5-year, $14 million contract to acquire a commercial off-the-shelf (COTS) EHR system. According to the Coast Guard's EHR business case, the system was to provide ambulatory services, including online management of patient health records; patient scheduling and billing services; dental

[13]A graphical user interface is a computer program designed to allow a computer user to interact easily with the computer typically by making choices from menus or groups of icons. In this regard, Coast Guard's PGUI software allows CHCS to be easier to understand and use.

and radiology modules; management of prescribed medications and tracking laboratory orders, among other capabilities.

However, while working to implement the COTS EHR system, HSWL staff determined that many other Coast Guard health care-related IT systems were outdated and also needed modernization. As a result, the HSWL Directorate began an effort to expand the original EHR modernization effort to integrate these other necessary and outdated services. This expanded project was called IHiS.

According to the HSWL Directorate, IHiS was to provide additional services such as work-life and safety data management, work-life case management, wireless access, and an integrated patient portal that was intended to allow patients to access their medical records at any time. The project consisted of various contracts with 25 different vendors and was estimated to cost approximately $56 million to implement, which included the original $14 million COTS EHR contract.

HSWL staff stated that, at the time that the IHiS project was being planned and designed, the Department of State was also planning to develop an EHR system. In order to reduce the overall cost to both parties, in 2012, the Department of State signed an interagency agreement with the Coast Guard to utilize IHiS for that department's personnel. The system was to be implemented in phases with beta testing at two to three selected Coast Guard clinics in October 2015, and then subsequent implementation at the other clinics, sick bays, and Department of State locations. However, on October 19, 2015, the Coast Guard decided to terminate the IHiS project and decommissioned PGUI in 2015 and CHCS in 2016.

The Coast Guard Attributed IHiS Termination to Financial and Other Risks, after Spending Approximately $60 Million on the Project

According to the Director of HSWL, who was appointed to the position in August 2015, financial, technical, schedule, and personnel risks led the Coast Guard's EOC[14] to decide to terminate the IHiS project. Specifically, the Director of HSWL provided us a written summary of information on the IHiS project risks that she said she had verbally communicated to the EOC during meetings on September 24, 2015, and October 6, 2015. The financial risks that the Director presented were based on internal investigations initiated in January 2015 and May 2015 to determine whether the HSWL Directorate had violated the Antideficiency Act[15] by using incorrect funding sources and incorrect fiscal year funds for the IHiS project. In this regard, the Coast Guard ordered project management and contractor staff to cease work on IHiS until a determination was made regarding the antideficiency violation.[16]

In addition, the Director stated that she relayed technical risks to the EOC. These risks were identified in an e-mail in late August 2015 by Coast Guard project management staff who participated in the design and development efforts for IHiS. The Director and the related e-mail identified the following technical risks:

- **Lack of testing**. IHiS lacked an independent security assessment to verify that the system's security infrastructure was adequate. In addition, full interface testing with systems such as the Defense Eligibility Enrollment Reporting System had yet to be completed to ensure security and data integrity.
- **Limited system functionality**. The system that was to provide user verification and IHiS role management services was not yet complete.

[14]The EOC is an admiral/senior executive service-level group established to monitor major risks, address emergent issues, review acquisition phase exit criteria progress, and provide direction to cross-directorate teams to support the successful execution of major and non-major acquisitions.

[15]The Antideficiency Act prohibits federal employees from, among other things, making or authorizing an expenditure or obligation that exceeds the amount available in an appropriation or fund. 31 U.S.C. § 1341(a)(1)(A). See GAO, *Principles of Federal Appropriations Law, Vol. 3, 3rd ed., ch. 6, § C.1.,* GAO-06-382SP (Washington, D.C.: September 2008).

[16]The investigation for the funding sources was completed in November 2015, and the investigation for fiscal year funding was completed in February 2016. It was determined in both cases that no Antideficiency Act violation had occurred. In this report, we are not assessing or commenting on the Antideficiency Act claims relevant to this issue.

In addition, Coast Guard workstations could not yet access IHiS from the network and the patient portal lacked two-factor authentication.[17] Further, the service that was to register new IHiS users in the system had yet to be completed.

The Director also presented schedule and personnel risks to the EOC:

- **Delays in the implementation timeline.** The Director stated that between August 2015 and September 2015, she requested that the DOD's Defense Health Agency Solution Delivery IT team[18] independently validate the IHiS timelines and the status of the project. The Director said she requested this review because of the technical risks identified in the August 2015 e-mail and concerns as to whether IHiS would be ready to be piloted at the first clinic in the fall of 2015. According to the Director, the Defense Health Agency team projected the timeline for the first clinic implementation to be approximately 1 year later than originally estimated. The Director added that Defense Health Agency team members stated that the timeline was delayed, in part, because critical IHiS interfaces and workflows were not complete or operational. The Director told us that these estimations were provided by the Defense Health Agency team verbally and that the team did not provide the Coast Guard any written documentation outlining its findings.
- **Changes in project management staff**. Although HSWL staff had been managing the IHiS project since it was initiated in 2010, C4&IT was directed to assume the oversight responsibilities for IHiS implementation in May 2015 due to concerns about the project's adherence to established governance processes raised by the internal investigators looking into the potential Antideficiency Act violations. By

[17]Authentication systems typically rely on one or more of the following factors: something you know (for example, a password); something you have (for example, an ID badge or a cryptographic key); and something you are (for example, a fingerprint or other biometric data). Two-factor authentication refers to the use of more than one of these factors. The strength of authentication systems is largely determined by the number of factors it uses. Implementations that use two factors are considered to be stronger than those that use only one factor, while systems that incorporate all three factors are stronger than systems that incorporate only two.

[18]According to its website, the Defense Health Agency is a joint, integrated combat support agency that enables the Army, Navy, and Air Force medical services to provide a medically ready force and ready medical force to combatant commands in both peacetime and wartime. The Solution Delivery Division within the Defense Health Agency is to deliver IT solutions to the Military Health System through acquisition program management, process re-engineering, information translation and sharing, training, and integration activities in order to support and advance the delivery of health care to its patients.

August 2015, the key project management personnel that had overseen the project since 2010 had been removed. According to C4&IT staff, IHiS was cancelled during the transition of project managers. As a result of the changes in staff, one vendor noted that it was unclear as to who were stakeholders, responsible parties, and decision makers.

According to the Director, these risk factors had demonstrated that the project was far from ready for deployment and that continuing IHiS could cause significant stewardship and reputational harm to the Coast Guard. As a result of the risks presented by the Director, the EOC members made the decision to cancel IHiS, and did not consider any other alternatives to its cancelation.

Subsequent to the project's cancelation, the Deputy Commandant for Mission Support conducted an analysis of the amount of money that had been obligated for and spent on the project. According to the analysis, which included obligations and expenditures from September 2010 to August 2017, the Coast Guard had obligated approximately $67 million and, of that amount, had spent approximately $59.9 million on the IHiS project at the time of its cancelation. Further, according to Office of Budget and Programs staff members, no equipment or software from the IHiS project could be reused for future efforts.

In addition, according to senior staff within the Acquisition Directorate, the Coast Guard continued to pay millions of dollars to vendors over 2 years after the project's cancelation to satisfy existing contractual obligations. For example, according to staff within the Acquisition Directorate:

- $102,993 was paid in November 2017 to one vendor for leased equipment that was damaged or missing, as part of closing out the contract.
- $460,352 was paid in November 2017 to an equipment vendor because the Coast Guard was obligated to do so after it had exercised the contract option period just prior to canceling IHiS.
- Approximately $872, 000 was paid to various vendors by November 2017 as part of closing out other contractual obligations for items such as software licensing and support and a data storage center.
- Approximately $2.4 million is to be paid to one vendor by February 2018 for software and licensing products.
- Approximately $2.8 million is to be paid by February 2018 for removal and shipment of equipment.

However, the amount spent on the project is likely underestimated because the Coast Guard's analysis of spending did not include labor costs for the agency's personnel (civilian or military) who spent approximately 5 years managing, overseeing, and providing subject matter expertise on the project. It also did not include any travel costs incurred by these personnel.

The Coast Guard Could Not Demonstrate Effective Project Management, Lacked Governance Mechanisms, and Did Not Document Lessons Learned for the IHiS Project

The Coast Guard could not demonstrate that it effectively managed and oversaw the IHiS project prior to its discontinuance. Specifically, although the Coast Guard was to follow the SDLC Practice Manual to guide its management and oversight of the project, the agency could not provide complete evidence that it had addressed 15 of the 30 SDLC practices we selected for evaluation. In addition, project team members provided inconsistent explanations regarding whether or not documentation existed to demonstrate the actions taken to manage and oversee the IHiS project. Further, although the Coast Guard developed charters for various governance boards to provide project oversight and direction, the boards were not active and the Chief Information Officer (CIO) was not included as a member of the boards, further contributing to a lack of key governance mechanisms for IHiS. Finally, the Coast Guard did not document and share lessons learned from the failed project to help prevent similar outcomes for future IT projects.

The Coast Guard Could Not Demonstrate That Selected Project Management Practices Were Addressed

In an effort to institute disciplined, repeatable practices for IT development and acquisition, the Coast Guard developed the *SDLC Practice Manual*, which establishes the seven-phase methodology for developing the Coast Guard's Assistant Commandant for C4&IT systems, such as IHiS. The practice manual is intended to guide project management teams through a progression of activities for managing and overseeing IT projects from conceptual planning to disposition. (Appendix II provides a discussion of each SDLC phase included in the practice manual and the 30 selected practices that we evaluated.)

Although IHiS was to adhere to the SDLC practices established in the manual, the Coast Guard could not demonstrate that the staff providing day-to-day management of the project had always done so. Specifically, of the 30 selected project management practices that we evaluated for

the initial four SDLC phases of IHiS[19]—Conceptual Planning, Planning and Requirements, Design, and Development and Testing—Coast Guard officials provided documentation that the project management team fully addressed 15 practices and partially addressed 5 practices. The agency could not provide documentation that the project team had addressed 10 other practices. Table 1 provides a complete listing of the SDLC project management practices that we selected for evaluation and the extent to which the Coast Guard could demonstrate that it completed each practice.

Table 1: Extent to Which the Coast Guard Demonstrated the Completion of Selected Systems Development Life Cycle (SDLC) Project Management Practices

SDLC phases and practices	GAO assessment
Phase 1: Conceptual Planning	
Assign project manager and asset manager.	●
Identify sponsor.	●
Develop the initial business case. This includes information relating to background, system justification, project risk management, rough timeline, and benefits.	●
Validate alignment with enterprise architecture.	○
Develop the initial acquisition strategy. During this step, the funding source for the project should be identified, at least through the Planning and Requirements phase, and a rough order of magnitude cost estimates should be provided.	●
Designate the system as a Command, Control, Communications, Computers, and Information Technology (C4&IT) system.	●
Obtain phase exit approval. A phase exit approval memorandum will be prepared by the appropriate commandant and returned to the sponsor to indicate the completion of the phase and the approval to move on to the next phase.	○
Phase 2: Planning and Requirements	
Complete a SDLC tailoring plan. The plan provides a clear and concise listing of SDLC process requirements throughout the entire system lifecycle, and facilitates the documentation of calculated deviations from standard SDLC activities, products, roles, and responsibilities from the outset of the project.	●
Create an initial project management plan that, at a minimum, contains a project description, work breakdown structure, project schedule/milestones, tools and methodologies, resource estimates which include a life cycle cost estimate, communication plan, project standards and procedures, and a listing of personnel assigned to the SDLC roles.	◐
Develop a project risk management plan that includes a list of vulnerabilities and recommended measures to overcome or lessen project risks.	●

[19]The remaining three phases—Implementation, Operations and Maintenance, and Disposition—were not applicable to the project as it was canceled prior to system implementation.

SDLC phases and practices	GAO assessment
Conduct a cost benefit analysis.	●
Document functional requirements.	●
Review external mandates.	●
Create the initial integrated logistics support plan. Major sections of the plan include the configuration management plan, data management plan, records management plan, and quality assurance plan.	○
Create the initial training plan.	●
Develop the information assurance plan, which is to include information security controls that are intended to ensure information integrity, authentication, confidentiality, and non-repudiation.	○
Designate system development agent and system support agent.	●
Obtain phase exit approval.	●
Phase 3: Design	
Develop the detailed system design. It should specify the operating system, architecture components, timing and sizing, external and internal interfaces, inputs and outputs of each subsystem, administrative activities, and security and auditing needs, and address all functional requirements.	◐
Develop the operational analysis plan. This plan should include system performance measures in terms of meeting the mission or organizational goal(s), meeting the needs of the user from an operational perspective, technical viability of the system, system availability, system reliability, and system response time. The plan should also include system operating measures (i.e., reliability, maintainability, availability, training, user satisfaction, and effectiveness of technology in providing desired functionality), and system support measures that capture the level of effort necessary to support the system and provide indications as to whether customer inquiries are being addressed in a timely and effective manner.	◐
Hold review sessions with the user community. The review sessions should include participation from support and training communities to ensure that all functional requirements were sufficiently met by the design.	○
Develop contingency and disaster recovery plans.	○
Complete the privacy impact analysis.	○
Create the test and evaluation master plan. The plan should document the scope, content, methodology, sequence, management of, and responsibilities for test activities. It should also describe the test activities of the subsystem integration test, the system test, and security testing in progressively higher levels of detail as the system is developed. Testing activities documented within the plan may include test cases, test scripts, and test scenarios.	◐
Test the system design in accordance with the operational test and evaluation plan and capture design test results in the test and evaluation master plan.	○
Obtain phase exit approval.	○
Phase 4: Development and Testing	
Conduct system testing.	○
Develop system documentation. This should include system manuals, user manuals, and diagrams, among other things, to be used or referred to during the Operations and Maintenance phase to reflect “as built” status.	◐
Prepare the implementation plan. This plan should describe how the system will be deployed in the operational environment; translate business needs into key activities (i.e., installation, training, verification, and monitoring); specify an implementation schedule; and identify specific personnel, system, interface, and site requirements.	●
Obtain authority to operate (ATO). The ATO is required prior to deploying a pilot in the production environment. By signing the ATO, the authorizing official accepts the security risks of the system.	●

SDLC phases and practices	GAO assessment
Phase 5: Implementation	
Not applicable as the system was canceled prior to implementation.	N/A
Phase 6: Operations and Maintenance	
Not applicable as the system was canceled prior to implementation.	N/A
Phase 7: Disposition	
Not applicable as the system was canceled prior to implementation.	N/A

Legend:

● = The Coast Guard provided documentation that demonstrated that the IHiS project satisfied all of the elements of the required SDLC project management practice.

◐ = The Coast Guard provided documentation that demonstrated that the IHiS project satisfied some but not all elements of the required SDLC project management practice.

○ = The Coast Guard could not provide documentation that demonstrated that the IHiS project satisfied any of the elements of the required SDLC project management practice.

Source: U.S. Coast Guard SDLC Practice Manual (criteria) and GAO (analysis of agency-provided data). | GAO-18-59

Conceptual Planning Phase

For this phase, the Coast Guard demonstrated that steps had been taken to address five of the seven selected project management practices for IHiS. Specifically, it assigned project management roles, such as the project manager, asset manager, and the system's sponsor. The agency also documented the initial IHiS business case and acquisition strategy, as well as the designation memorandum that identified IHiS as a C4&IT system.

However, the Coast Guard could not demonstrate that the project management team had validated the project's alignment with the agency's enterprise architecture and that the project had received the required phase exit approval. As a result, the Coast Guard could not provide evidence that the necessary steps were taken to ensure that the project would align with the agency's business objectives and that project management staff had received approval to proceed to the next SDLC phase.

Planning and Requirements Phase

For this phase, the Coast Guard demonstrated that 8 of the 11 selected project management practices were performed for the IHiS project. Specifically, the agency provided evidence that it had completed the tailoring plan that detailed the SDLC processes that would be required throughout the IHiS system's lifecycle, developed an initial risk management plan that included a list of vulnerabilities and the measures to overcome or lessen them, and conducted a cost benefit analysis. The Coast Guard also documented functional requirements; reviewed external

mandates, such as those mentioned earlier;[20] created an initial training plan; and designated the system development and system support agents. Finally, the Acting CIO approved the project to move to the next phase and stated in a memorandum that the project had met all the requirements of the planning and requirements phase.

However, the Coast Guard could not demonstrate that it had fully completed all of the requirements of this phase. For example, the Coast Guard provided documentation that partially met the requirement to develop a project management plan. Specifically, the agency created a project management plan that included certain required elements, such as a project description, work breakdown structure, and a life cycle cost estimate. However, it did not complete other required elements. Specifically, although the Coast Guard developed a project schedule for IHiS, it was not well-constructed,[21] which made the overall quality of the IHiS schedule unreliable. For example, the IHiS schedule allowed for many activities to slip a significant number of days before impacting the dates of key events. Further, the Coast Guard could not demonstrate that it had created a communication plan—another element of the project management plan—that is essential to identifying how system development progress is to be communicated across the project management team.

The Coast Guard also could not demonstrate that two other selected practices were addressed. Specifically, the agency could not provide an integrated logistics support plan that is intended to document processes for ensuring IHiS data management and records management, among other things. In addition, the Coast Guard could not demonstrate that it had developed an information assurance plan that is intended to articulate the information security controls required to ensure the availability, integrity, authentication, and confidentiality of the patient health information that was to be stored in IHiS. As a result, the Coast Guard could not demonstrate that it had performed key steps to construct

[20]Executive Order 13335, *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator* (Apr. 27, 2004); and Executive Order 13410, *Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs* (Aug. 22, 2006).

[21]According to our Schedule Assessment Guide, GAO-16-89G, the four characteristics of a high-quality, reliable schedule are that it is comprehensive, well-constructed, credible, and controlled. A schedule is well-constructed if all its activities are logically sequenced with the most straightforward logic possible.

a reliable schedule for IHiS, plan for how the project's progress was to be communicated to key stakeholders, ensure appropriate data and records management for information stored in IHiS, and plan for the controls necessary to secure patient health information.

Design Phase

The Coast Guard demonstrated that actions had been taken to partially address three of the eight selected project management practices for the design phase. In this regard, the agency partially addressed the requirement to develop a detailed system design. Specifically, the system design documentation included a description of the operating system, external and internal system interfaces, inputs and outputs of each subsystem, administrative components that are intended to connect systems, and system security requirements. However, the system design documentation did not include information on the system architecture components, system timing and sizing, and system auditing requirements. The documentation also did not address all IHiS functional requirements as required by the SDLC.

The Coast Guard also partially addressed the requirement to develop an operational analysis plan. For example, the plan included performance and operating[22] measures related to availability, maintainability, and training. It also included support measures related to system utilization, incident management, and problem management. However, the Coast Guard had not included mission-related performance measures; operating measures related to reliability, user satisfaction, and effectiveness of technology; and other system support measures related to change management.

In addition, the agency partially addressed the requirement to create the test and evaluation master plan. Specifically, the test and evaluation master plan included required elements, such as the scope, content, methodology, and sequence of testing, as well as the management of and responsibilities related to testing activities. However, the plan did not define activities for integration and security testing, both of which are intended to validate that the integrated system components function properly.

[22]According to the Coast Guard's operational analysis plan for IHiS, types of system operating measures include reliability, maintainability, availability, training, user satisfaction, and effectiveness of technology in providing desired functionality.

The Coast Guard could not demonstrate that five other selected practices were addressed for the IHiS project. In this regard, it could not demonstrate that the project team had:

- held review sessions with the user community to ensure that the requirements and the design were consistent with the new or enhanced business requirements;
- developed contingency and disaster recovery plans to document the steps necessary to continue IHiS operations in the event of a disruption;
- completed the privacy impact analysis to describe what information was to be collected by IHiS, why the information was being collected, intended use of the information, and how the information was to be secured, among other things;
- tested the system design to ensure that it would have met requirements and support business processes; and
- obtained exit approval for the design phase to demonstrate that all requirements of the phase were met.

As a result, no evidence was provided that the Coast Guard performed all of the required steps to translate detailed system requirements into the system design and develop plans for life cycle support, such as those that address contingencies, disaster recovery, and testing for IHiS.

Development and Testing Phase

The Coast Guard demonstrated that actions had been taken to address two of the four selected practices and partially addressed one practice for the development and testing phase. For example, the agency developed the IHiS implementation plan that specified key activities, such as system training and monitoring, and included a schedule of activities that were to be accomplished during implementation. In addition, the Coast Guard created a diagram of the IHiS system layout as part of its effort to address one practice—to develop system documentation. However, it could not demonstrate that other required system documentation, such as system and user manuals that specify how to use and operate the system, had been created.

Further, the Coast Guard could not demonstrate that it had conducted IHiS system testing, although the agency granted an authority to operate

(ATO)[23] and indicated in the ATO memorandum that the system had undergone some form of testing. The Coast Guard's SDLC specifies that system testing is to take place prior to the issuance of an ATO. However, according to a memorandum signed by the IHiS authorizing official, a short-term ATO was granted for the system on March 30, 2015, in an attempt to ensure there would be a functioning replacement system in place prior to the decommissioning of CHCS. Nevertheless, the Coast Guard could not provide complete evidence that it took the necessary steps intended to ensure that the system would function as expected, such as conducing system testing.

Relevant Documentation Was Often Not Available

Over the course of our review, Coast Guard project team members provided inconsistent explanations regarding the availability of documentation to support the project management activities for IHiS. For example, with regard to the SDLC practices that we identified as not having been implemented, the former IHiS project manager and a knowledgeable representative for the contractor responsible for providing engineering and acquisition technical assistance for IHiS stated that the agency had developed most of the supporting documentation which would demonstrate that actions consistent with the SDLC practices had been taken.

In addition, annotations within the IHiS acquisition strategy indicated that required SDLC artifacts, such as enterprise architecture documentation; plans for integrated logistics support, contingency, and disaster recovery; and a privacy impact assessment, among many others, were documented, available, and maintained within a document management tool. However, staff within the HSWL Directorate, the Office of Budget and Programs,[24] and the Office of Enterprise Applications

[23]The National Institute of Standards and Technology Special Publication 800-37 defines the ATO as the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls. According to the Coast Guard's *SDLC Practice Manual*, an ATO is required prior to deploying a pilot of the system in the production environment.

[24]The Office of Budget and Programs is responsible for reviewing and coordinating the planning and execution of current and proposed programs, including the determination of Coast Guard priorities for resource allocation, among other things.

Management[25] told us that the documentation either did not exist or could not be located because several of the key project management team members were no longer employees of the Coast Guard.

The absence of the various documents and other artifacts that would support the required SDLC activities raises doubts that the Coast Guard took the necessary and appropriate steps to ensure effective management of the IHiS project. Carrying out established procedures for effective management and oversight of IT projects will be important for supporting any system development and acquisition effort that the Coast Guard undertakes to implement a future EHR system.

The Coast Guard Lacked Governance Mechanisms for IHiS Oversight

According to the *IT Investment Management Framework*, efforts to build a foundation for IT governance involve establishing specific critical processes, such as instituting investment boards and controlling investments as they are developed.[26] In addition, we have long reported that federal IT projects have failed due, in part, to a lack of oversight and governance especially at an executive-level, such as the CIO.[27]

The Coast Guard documented charters for four governance bodies that were intended to provide oversight to the IHiS project:

- The Executive Steering Committee was to provide executive oversight of the design, implementation, operation, and long term direction for IHiS. Responsibilities of the committee were to include monitoring the overall acquisition, integration, and operation of IHiS; authorizing major changes in the project's objectives, scope, and requirements; and reviewing the reliability, availability, and affordability of the project, among other things. Members of the committee were to include representatives from the Coast Guard's HSWL Directorate,

[25]The Office of Enterprise Applications Management provides programmatic oversight and portfolio management of enterprise-wide human resources, financial and operations IT systems.

[26]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

[27]GAO, *Information Technology: Sustained Management Attention to the Implementation of FITARA Is Needed to Better Manage Acquisitions and Operations*, GAO-17-686T (Washington, D.C.: June 13, 2017).

the Office of Enterprise Applications Management, and Department of State representatives.[28]

- The User Group was to make recommendations to the IHiS Program Management Office on functionality and system design and to ensure that decisions were based on end-user needs. Responsibilities of the group were to include making suggestions on improving IHiS for the user, participating in planning for future changes or upgrades to the system, and evaluating strategies to maintain and improve system efficiency. The IHiS project manager was to serve as chair of the group, and the Coast Guard and Department of State were to nominate user representatives from each functional area of IHiS as additional group members.
- The Change Control Board was to evaluate change proposals in regard to technical, user, and cost impact to the system and recommend change requests to the IHiS baseline. Members of the board were to include representatives from the Coast Guard's Office of Enterprise Applications Management, the Business Operations Division, and the Department of State.
- The System Security Committee was to manage the risk to IHiS and identify and mitigate security vulnerabilities. Responsibilities of the committee were to include reviewing IHiS security configurations, changes to those configurations, and proposed changes to IHiS to ensure that the system's security would not be compromised. Members of the committee were to include representatives from the Coast Guard's Office of Enterprise Applications Management, the Business Operations Division, and Department of State security and privacy representatives.

While the Coast Guard chartered these various governance bodies for IHiS oversight, the agency could not provide evidence that the boards had ever been active in overseeing the project prior to its cancelation. As a result, the IHiS project lacked important oversight mechanisms to ensure the project's success.

In addition, the CIO (Deputy Assistant Commandant for C4&IT) was not included as a member of any of the IHiS governance bodies. According to a memorandum signed by the Acting CIO in 2011, C4&IT was responsible for ensuring that the IHiS project was compliant with SDLC

[28]The Coast Guard established an interagency agreement in December 2011 to share IHiS with the Department of State.

requirements. However, the Coast Guard could not provide evidence that demonstrated how C4&IT and the CIO were involved in ensuring compliance with the requirements. Taking steps to fully implement governance boards that include the CIO will be important to the Coast Guard's oversight efforts in implementing a future EHR system and may decrease the risk of IT project failure.

The Coast Guard Did Not Document Lessons Learned from the IHiS Project

We developed the *IT Investment Management Framework* that stresses the importance of identifying lessons learned to support future investment decisions.[29] We have also previously reported that mechanisms for documenting, sharing, and disseminating lessons learned serve to communicate acquired knowledge more effectively and ensure that beneficial information is factored into planning, work processes, and activities. Lessons learned provide a powerful method of sharing good ideas for improving work processes, facility or equipment design and operation, quality, safety, and cost-effectiveness. They can be based on positive experiences or on negative experiences that result in undesirable outcomes, such as the cancelation of the IHiS project. Additionally, it is important to disseminate lessons learned since lessons are of little benefit unless they are distributed and used by people who will benefit from them.[30]

Although Coast Guard officials stated that lessons learned had been identified throughout the process of developing IHiS, as of 2 years after its cancelation, the agency had not documented and shared any lessons learned from the project and does not have established plans for doing so. According to an official from the Office of Budget and Programs, the Coast Guard had not yet documented lessons learned because the agency views the lessons learned process as ongoing.

While the Coast Guard may view the lessons learned process as ongoing, the IHiS project was canceled in 2015, and it is important to document and share the lessons already identified so that this beneficial information can be factored into the planning activities for future systems and projects. Until the Coast Guard takes steps to document and share identified lessons learned with individuals charged with developing and

[29]GAO-04-394G.

[30]GAO, *NASA: Better Mechanisms Needed for Sharing Lessons Learned,* GAO-02-195 (Washington, D.C.: Jan. 30, 2002).

acquiring its IT systems, opportunities to protect future systems against the recurrence of mistakes that contributed to the failure of IHiS will likely be missed.

The Coast Guard Is Managing Health Records Using a Predominately Paper Process; Many Challenges Hinder Service Delivery

In the absence of an EHR system, the Coast Guard currently relies on a predominately paper health record management process to document health care services for its nearly 50,000 military members. After canceling the IHiS project in October 2015, the agency could not return to managing health records using its legacy electronic capabilities because PGUI was decommissioned in 2015 and CHCS was decommissioned in January 2016.[31] Thus, the Coast Guard directed clinics and sick bays to remove relevant information from CHCS and PGUI and maintain all health records for its members using a predominately paper process.

The Coast Guard supplements its current paper process by using applications that various other agencies operate and maintain. For example, the Coast Guard uses the Navy's Medical Readiness Reporting System to, among other things, track immunizations, periodic health assessments, dental exams, dental status, and required physical exams. In addition, the agency uses the Army's Aeromedical Electronic Resource Office electronic tracking system to document aviation physical exams and aero medical summaries.[32] However, while these systems hold valuable information, they are separate applications requiring separate logins and do not encompass comprehensive Coast Guard health beneficiary information.

[31]According to the HSWL Director, CHCS was decommissioned due to its inability to comply with the 10th revision of the International Classification of Diseases code requirements. These codes are the standard code set used in the United States, including in the Medicare and Medicaid programs, for documenting patient medical diagnoses and inpatient medical procedures. All health care providers, health care clearinghouses, and health plans were required to transition to the 10th revision of the International Classification of Diseases codes, called International Classification of Diseases-10.

[32]Other systems include the Defense Enrollment Eligibility Reporting System—a program that verifies all authorized DOD and Coast Guard beneficiaries and employees; the Disease Reporting System Internet—a system that serves as the official repository for reportable medical events for the Coast Guard, Army, Navy, and Air Force; the Health Artifact and Image Management Solution—a repository used to digitally store paper health records of Coast Guard members who are separating or retiring from the Coast Guard; and the Joint Legacy Viewer—an application that provides a read-only view of health information from DOD, VA, and private sector partners. Some of the Coast Guard providers have access to AHLTA by local DOD medical treatment facilities to review patient health encounter data, enter in referrals, and order labs and radiology.

Currently, the Coast Guard's clinical staff (i.e., clinic administrators[33] and clinicians[34]) are to generally perform the following steps to process each paper health record:

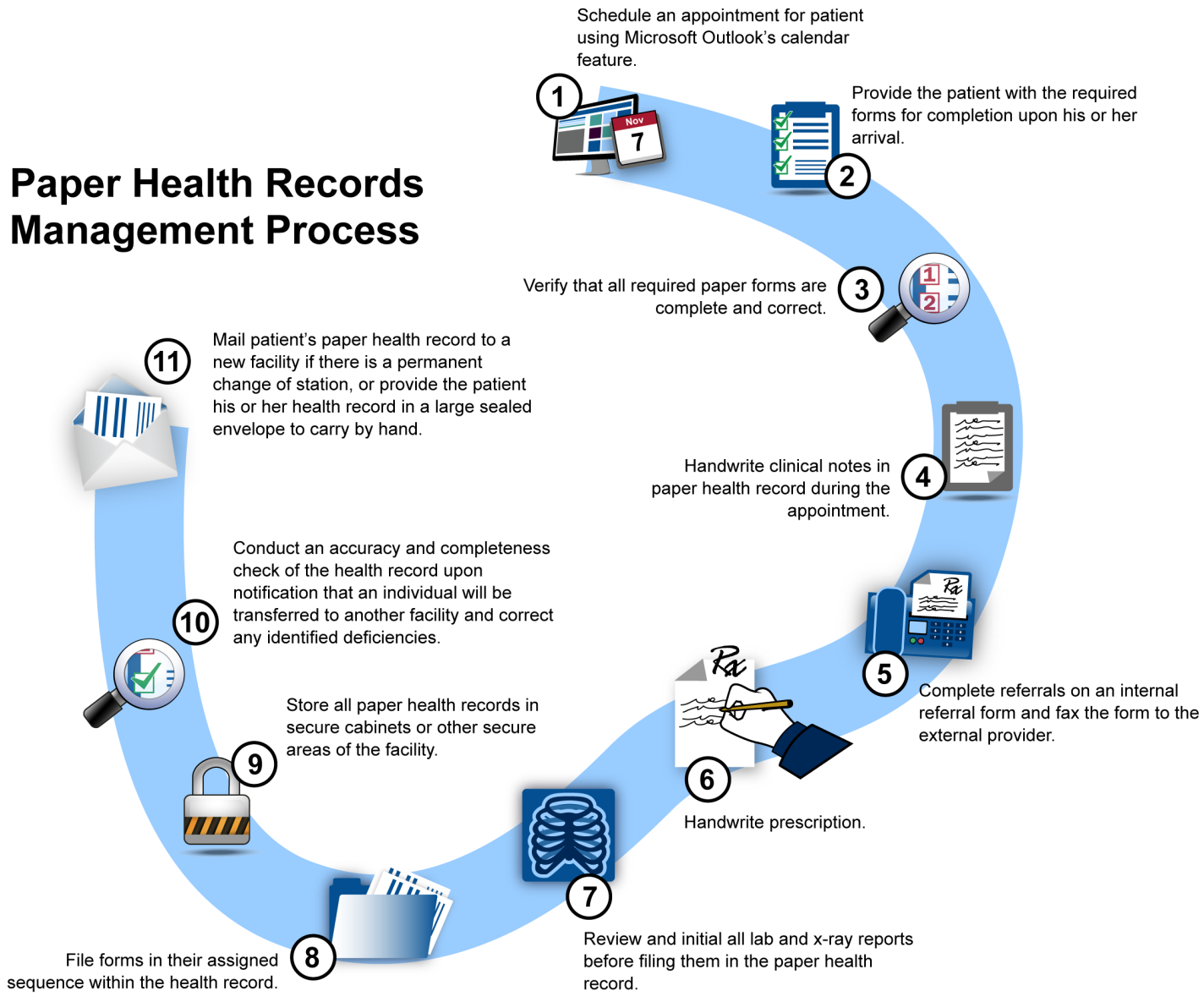
- Schedule an appointment for patient using Microsoft Outlook's calendar feature.
- Provide the patient with the required forms for completion upon his or her arrival.
- Verify that all required paper forms are complete and correct.
- Handwrite clinical notes in a paper health record during the appointment.
- Complete referrals on an internal referral form and fax the form to the external provider.
- Handwrite prescription.
- Review and initial all lab and x-ray reports before filing them in the paper health record.
- File forms in their assigned sequence within the health record.
- Store all paper health records in secure cabinets or other secure areas of the facility.
- Conduct an accuracy and completeness check of the health record upon notification that an individual will be transferred to another facility and correct any identified deficiencies.
- Mail patient's paper health record to a new facility if there is a permanent change of station, or provide the patient his or her health record in a large sealed envelope to carry by hand.

Figure 1 generally depicts the required steps for managing paper health records.

[33]For the purposes of our report, a clinic administrator refers to a Coast Guard clinic administrator, health services technician, or clinic supervisor.

[34]For the purposes of our report, a clinician refers to a Coast Guard physician, physician assistant, or contract physician assistant.

Figure 1: General Steps That the Coast Guard's Clinical Staff Are to Follow to Process Paper Health Records



Source: GAO analysis of United States Coast Guard data. | GAO-18-59

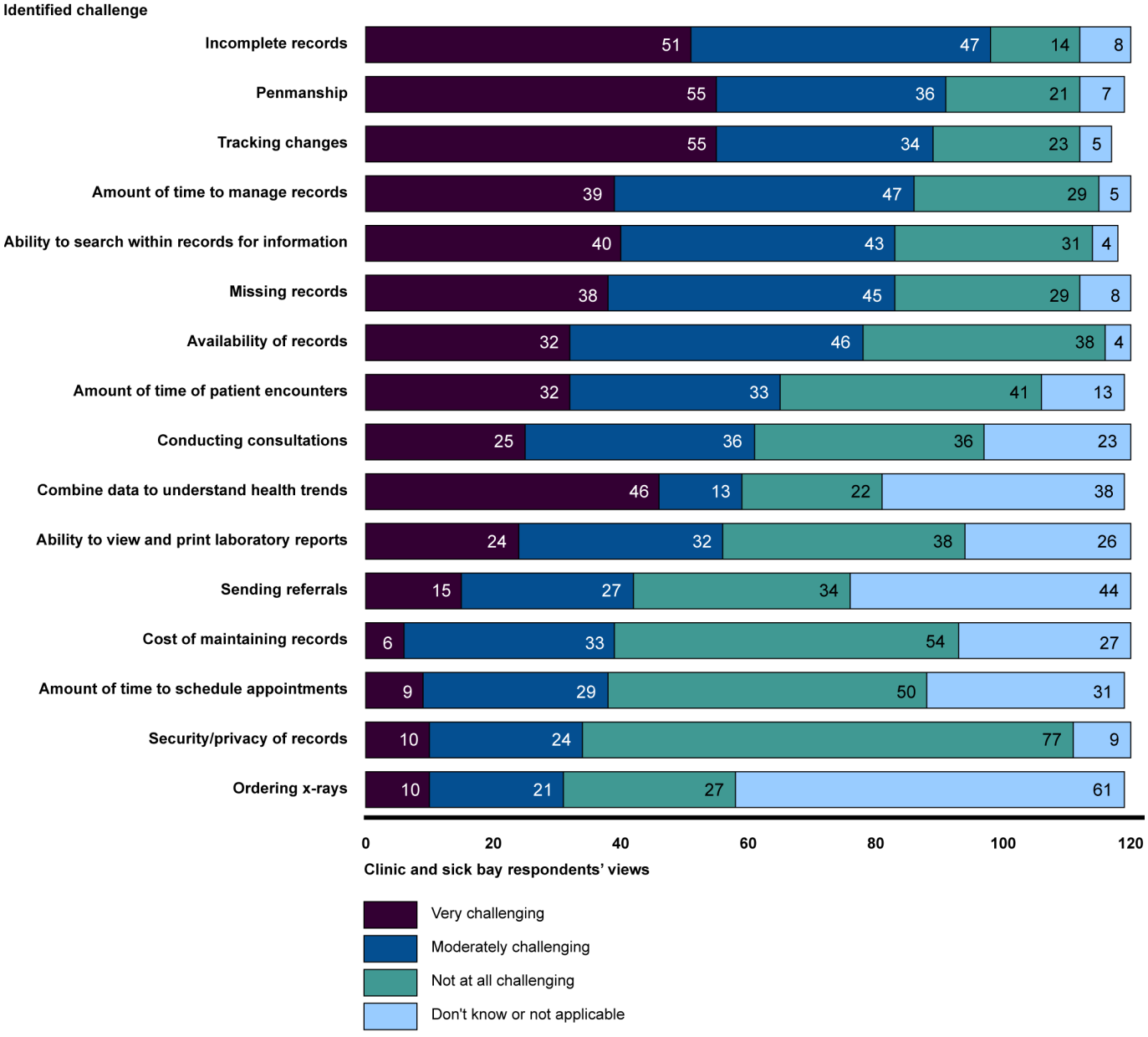
The Coast Guard Faces Numerous Challenges in Managing Its Paper Health Records and Has Adopted a Number of Manual Steps to Deliver Services

In response to our survey, the 12 HSWL Regional Managers identified a number of challenges that clinics and sick bays in their regions had experienced in managing and maintaining paper health records.[35] These challenges were grouped into 16 categories. Further, the 120 clinic and sick bay administrators that subsequently responded to a separate survey reported varying degrees to which they viewed each category as challenging.[36] Figure 2 provides the clinic and sick bay respondents' views of the challenges.

[35]We surveyed all 12 Regional Managers and received a response from all 12 managers.

[36]We sent surveys to all 166 local clinic and sick bay administrators and received a response from 120 of the 166 administrators. See appendixes III and IV for survey questions.

Figure 2: Clinic and Sick Bay Survey Respondents' Views of the Challenges Identified by Regional Managers in Managing and Maintaining Paper Health Records



Source: GAO survey data. | GAO-18-59

The following summarizes clinic and sick bay responses for each identified challenge with managing and maintaining paper health records:[37]

Incomplete records. Ninety-eight (82 percent) of the respondents reported incomplete records[38] as challenging. In this regard, 34 of the survey respondents reported that not all CHCS and PGUI records were printed out and included in patients' paper health records as required before the systems were retired; therefore, they had no way to ensure the patients' paper records were complete. According to one respondent, paper records are also often incomplete due to parts of the record being dispersed across different medical facilities, thus, making it difficult to put together a complete patient history and sometimes resulting in the need to repeat testing and treatment of patients.

Penmanship. Among the 91 (76 percent) survey respondents that reported penmanship as challenging, several noted that it is difficult for staff to read illegible handwritten medical notes. This, in turn, results in difficulty determining the accurate diagnosis, the required prescription, or a referral.

Tracking medications. According to 89 (76 percent) of the respondents, it is challenging to track medications without an EHR. For example, one administrator stated that the lack of an EHR makes the management of patient medication use difficult, as staff are unable to verify what medications a patient is taking, what medications have been prescribed from an outside location, and/or the effectiveness of medications. Another administrator stated that staff members rely heavily on patients to remember what medications they are taking—potentially causing harm if patients cannot remember what medications they are taking and the medications have dangerous interactions.

Amount of time to manage records. According to 86 (72 percent) of the respondents, managing paper health records is challenging and requires more time for staff to complete and file paperwork. Several respondents

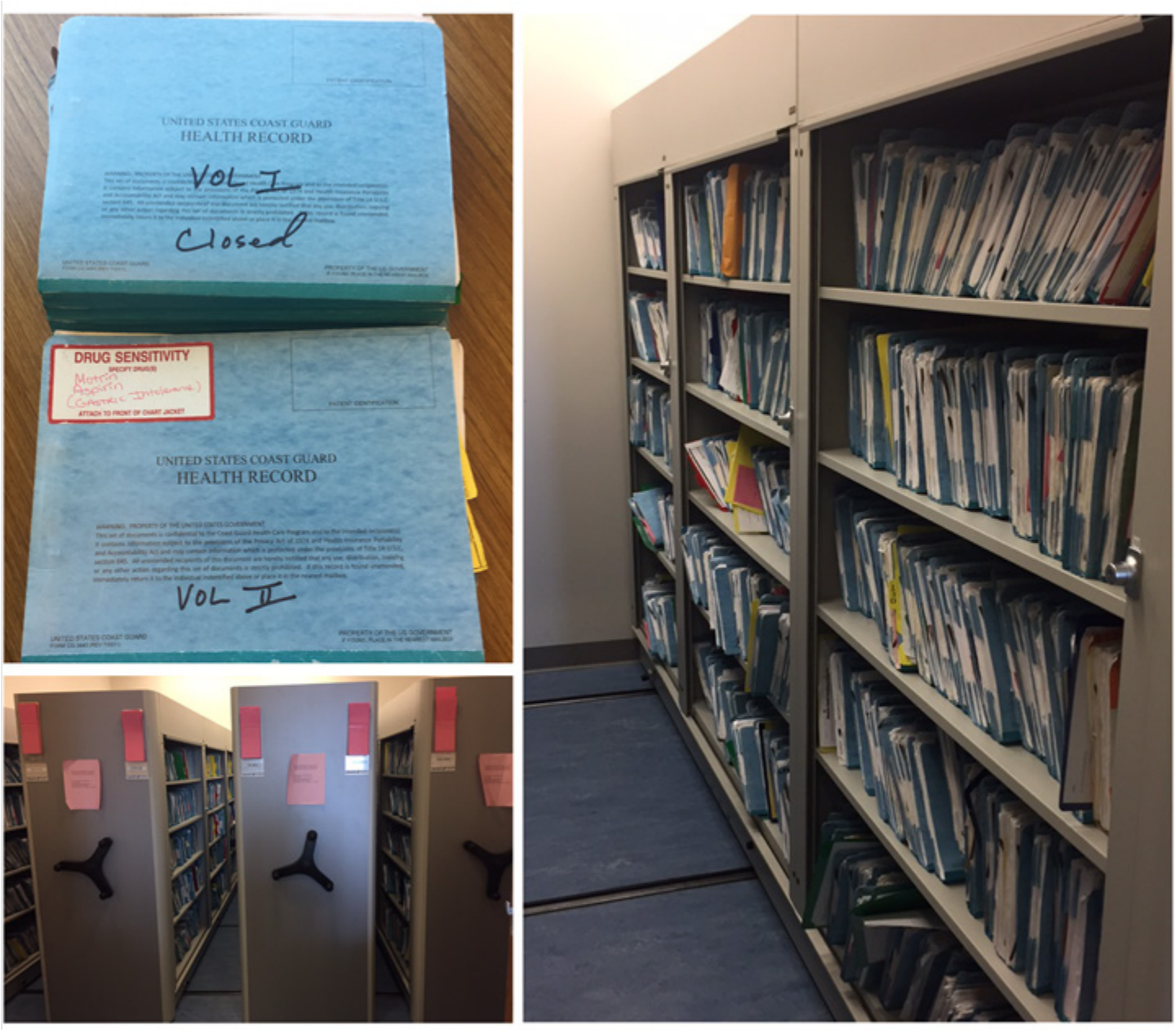
[37]For the purpose of summarizing the responses to the identified challenges, each survey response of either very or moderately challenging was grouped together and is reported as "challenging."

[38]For the purposes of our survey, a paper record is incomplete when a patient's health record does not contain all the necessary health information, including the history of clinic visits, prescribed medications, or lab results.

stated that the size of the paper health records has increased, resulting in additional time required to review and file records.

Ability to search within records. Eighty-three (70 percent) of the respondents reported the ability of clinical staff to search within paper health records for information as challenging. For example, one respondent stated that providers must flip through individual pages of a record to search for necessary information. Another respondent reported that some patients have up to three volumes of a health record and it can take up to 2 or 3 days to find requested information if the patient does not recall when or where the medical care was performed. Figure 3 shows a large paper health record and the multiple storage cabinets used to store them, which illustrates the difficulty in manually searching for information within the records.

Figure 3: Examples of a Coast Guard Paper Health Record with Multiple Volumes and Storage Cabinets



Source: United States Coast Guard photos. | GAO-18-59

Missing records. Eighty-three (69 percent) of the survey respondents stated that missing records are challenging. According to one administrator, repeat evaluations that may not be required for chronically ill patients are being conducted due to missing records. Another administrator stated that information can often get misfiled in the record of a patient with a similar name.

Availability of records. Seventy-eight (65 percent) of the respondents reported that the availability of records is challenging. For example, one administrator reported that many records are located in different locations, making it difficult to access the necessary information. Another administrator stated that delays occur when clinic staff have to wait for patients to bring records in for review or wait for updated notes from a previous location.

Amount of time for patient encounters. According to 65 (55 percent) of the respondents, the lack of an EHR has resulted in an increase in the amount of time required to check-in patients, complete patient appointments, and enter information in the patient record. According to one administrator, clinical documentation has to be completed by hand and some clinicians wait until the end of the day to complete notes. Another administrator reported that the clinician stays after the clinic closes to complete notes.

Conducting consultations. Sixty-one (51 percent) of the respondents reported conducting consultations with paper records as challenging. Several administrators stated that patient information is faxed or scanned and submitted for the consulting provider to review. According to one administrator, there are times when documentation must be faxed or scanned multiple times in order to produce a legible copy, resulting in increased time spent gathering and submitting information.

Health trends. According to 59 (50 percent) of the respondents, the use of paper records makes combining data to understand population health trends challenging. According to one survey respondent, accomplishing this without an EHR requires manually searching through every paper health record.

Ability to view and print laboratory reports. Fifty-six (47 percent) of the survey respondents reported that the inability to view and print laboratory reports without an EHR is challenging. One administrator stated that their clinic could view and print the results from one particular laboratory, but if a patient received services from any other lab the clinic staff would have

to request that the patient bring the laboratory results to the clinic. Another administrator stated that it could take 2 or more days to receive requested lab results because there was no way to easily obtain them via a centralized system.

Sending referrals. Forty-two (35 percent) of the respondents stated that sending referrals is challenging. One administrator reported facing challenges with faxed referral forms not being received after obtaining a fax confirmation. Another respondent reported having to spend an increased amount of time on the referral process with each referral necessitating at least 20 minutes to complete the required forms and fax them to the external provider—with 10–25 referrals being sent each day.

Cost of maintaining records. Thirty-nine (33 percent) of the respondents reported that the cost of maintaining paper health records is challenging. For example, one administrator reported that health records are frequently mailed to other medical locations or to the National Archives (for those separated or retired), which is a large expense for the Coast Guard. Another administrator stated that the time taken to gather paperwork, wait for civilian providers to send notes, and coordinate and execute health record updates is costly to the Coast Guard. Lastly, several administrators reported that expenditures for paper and printing products have increased due to the lack of an EHR. For example, one administrator reported that the clinic had increased its expenditure for paper by 50 percent.

Scheduling of appointments. Thirty-eight (32 percent) of the respondents reported that the time it takes to schedule appointments is challenging. One administrator stated that, due to the lack of a scheduling system, patient appointments are being scheduled using the Outlook calendar function, which is time consuming when there are network slowdowns or freezes during high rates of utilization. Another administrator reported that appointments are sometimes double scheduled or occasionally disappear from the calendar and, in one instance, a patient received an appointment reminder for an appointment that the patient had never scheduled.

Security/privacy of records. According to 34 (28 percent) of the respondents, the security and privacy of health records is challenging. One administrator reported that paper records are more prone to be within reach of individuals that should not have access to them because they are not stored in a secure EHR that has protections built in.

Ordering x-rays. Thirty-one (26 percent) of the respondents reported that the process for ordering x-rays is challenging. According to several administrators, the current process for ordering x-rays involves submitting a referral by fax, which takes additional time for processing and waiting for results to be returned by fax. Several administrators reported that it is difficult to know if all x-ray results have been received and filed.

The responding clinic and sickbay administrators described a range of alternative work-around processes that they have developed to help alleviate several of the challenges. Specifically, they reported having developed additional forms, tracking methods, and alternative processes, as well as having notified Coast Guard HSWL management of the challenges they face.

Regarding developing forms, approximately 31 percent of the survey respondents noted that they had developed additional forms in order to more easily obtain the information that they would have had available to them with an EHR in place. According to one administrator, these forms are based on the most common patient encounter needs and capture information such as medications, allergies, chronic issues, and family history. In addition, these administrators reported developing electronic file versions, such as a Microsoft Word document, of the standard health forms so that they can e-mail them to patients and reduce the number of paper forms that have to be completed by hand and scanned. According to the administrators, these steps help address handwriting and space challenges.

In addition, approximately 37 percent of the respondents reported developing tracking methods, such as Microsoft Excel spreadsheets and logs, to collect data and assist in tracking patient and provider information. One administrator reported that a spreadsheet was created to track patients with conditions that require monitoring, since there is no longer a system that has the data in one place. Another administrator reported creating a spreadsheet to track referrals, numbers of physicals, patient encounters, and medical readiness. Based on the survey responses, these tracking methods have helped address the challenges related to combining data to understand health trends, and tracking medications and referrals.

Further, 30 percent of the survey respondents noted that they have also developed alternative processes to mitigate some of the challenges with managing paper health records. For example, one administrator stated that the clinic started conducting weekly reconciliations of referrals to

ensure that all treatment records from outside referrals were obtained by the clinic and placed in the paper health record. Another administrator stated that the clinic had begun e-mailing patient encounter notes to the medical officer for review in an effort to ensure patient records are complete.

Finally, approximately 55 percent of the respondents reported that they have notified HSWL senior management of the challenges encountered with managing and maintaining paper records. According to an official within the Acquisitions Directorate, the Coast Guard plans to mitigate many of the challenges identified by the Regional Managers with a new EHR system initiative. However, these alternative processes may not provide sustained solutions to overcoming these challenges. Until Coast Guard implements a new EHR solution, the challenges inherent in a predominantly paper process will likely remain.

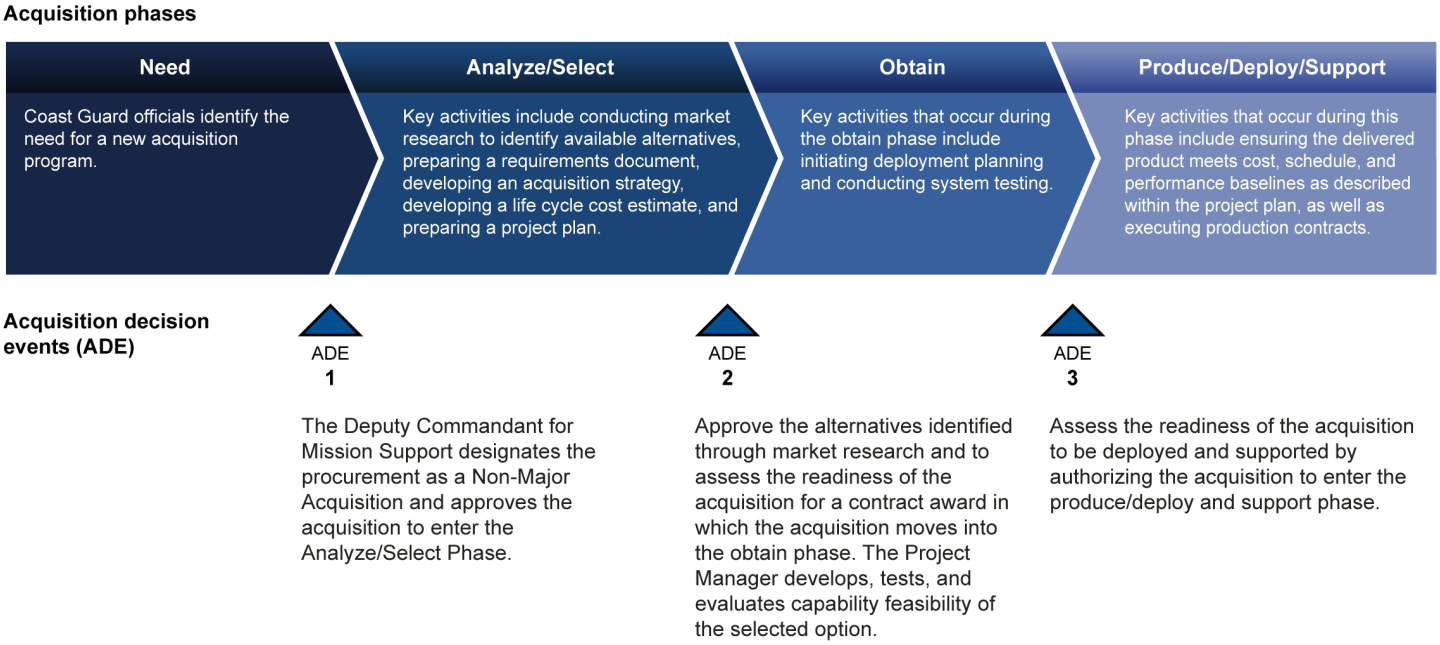
The Coast Guard Intends to Acquire a New EHR System, but Has Not Yet Chosen a Solution

The Coast Guard has begun taking steps to acquire a new EHR system referred to as the Electronic Health Record Acquisition (eHRa). According to the Acquisitions Directorate, the Coast Guard plans to manage and oversee the acquisition of eHRa through its non-major[39] acquisition process (NMAP), as described in its *Non-Major Acquisition Process (NMAP) Manual.*[40] The NMAP requires formal approval reviews at three discrete knowledge points called acquisition decision events (ADE) and includes three phases to assess the readiness and maturity of the acquisition. Figure 4 graphically represents the ADEs and phases of the NMAP. (Appendix V provides a more detailed discussion of each ADE and each of the three phases that make up the NMAP process.)

[39]According to the Coast Guard, a non-major acquisition is a procurement greater than $10 million in procurement costs and less than $300 million in life cycle costs. Major acquisitions are characterized as procurements above $300 million in life cycle costs.

[40]The Coast Guard implemented this process for non-major IT acquisitions in December 2012. It is intended to provide oversight of non-major acquisitions. As of August 2017, the Coast Guard was in the process of updating the NMAP. See Coast Guard, *Non-Major Acquisition Process (NMAP) Manual*, COMDTINST M5000.11B (Washington, D.C.: Dec. 31, 2012).

Figure 4: The Coast Guard's Acquisition Decision Events and Phases for Non-Major Acquisition Programs



Source: GAO analysis of Coast Guard's NMAP Manual. | GAO-18-59

Once the Coast Guard identifies the need for a new acquisition program, the program's sponsor is to seek ADE-1 approval. ADE-1 occurs when the program is designated as a non-major acquisition by the Deputy Commandant for Mission Support.[41] If an acquisition receives ADE-1 approval, it proceeds to the analyze/select phase of the NMAP. The analyze/select phase is the first of three phases of the process, and includes required work activities such as preparing a requirements document, conducting market research to identify available alternatives, developing an acquisition strategy, developing a life cycle cost estimate, and preparing a project plan.

The Coast Guard formally identified the need for a new EHR system on February 1, 2016, and obtained ADE-1 approval on February 13, 2016. Subsequent to the ADE-1 approval, the Coast Guard initiated the following activities associated with the analyze/select phase:

[41]The Deputy Commandant for Mission Support is responsible for lifecycle management of Coast Guard assets including ships, planes, buildings, and IT.

Requirements development. As part of its efforts to develop new system requirements for eHRa, the Coast Guard identified its capability gaps as a result of the lack of an EHR in a Capability Analysis Report. The report offered two courses of action to address the capability gaps: (1) business process re-engineering to enhance the current paper-based process, or (2) transition to a system-based solution. According to the Acquisitions Directorate, the Coast Guard plans to use the report to inform its effort in developing requirements for eHRa.

Market research. The Coast Guard issued a request for information in April 2017 to assess industry capabilities as part of market research for the new system. The request for information asked that the solutions fall into one of four categories that the Coast Guard was considering:

- Federal shared service. This option would allow the Coast Guard to use a system that is already in use by another federal agency. In addition, this option aligns with the Office of Management and Budget's Federal Information Technology Shared Services Strategy, issued in May 2012, which highlighted the prevalence of redundancy in federal IT systems.
- Managed by the Coast Guard, but externally hosted. This solution would require the Coast Guard to acquire a COTS system and manage its implementation. However, the system would be maintained by a vendor at an externally hosted data center.
- Commercial software as a service. This option involves purchasing commercial software for an EHR solution that is operated and maintained by a commercial vendor.
- In-house. With this solution, the Coast Guard would manage the implementation and maintenance of a COTS system with support from a commercial vendor.[42]

As a result of the Coast Guard's request for information, the agency collected cost, schedule, and capabilities information from 18 commercial

[42]According to an official from the Office of Budget and Programs, previously leased equipment and purchased software for the discontinued IHiS project will not be considered as part of an in-house managed implementation and maintenance solution. This is due to the fact that the equipment has now been repurposed by the commercial provider and purchased software was removed from the commercial servers after the project hosting agreement was canceled. In addition, although the Coast Guard purchased mobile iPad devices in support of IHiS, their pending obsolescence prohibits the reuse of those devices.

and government solution providers, including DOD and VA. The providers submitted proposed solutions ranging from $25 million to $163 million, including implementation and 10-year sustainment costs. The estimated timeline for the proposed solutions to reach full operational capability varied from 18 to 30 months.

The Coast Guard used the providers' responses to develop an alternatives analysis report that was completed in October 2017. The report recommended a solution based on performance, risk, cost, and schedule advantages. The report indicated that the Coast Guard plans to use the results of the alternatives analysis to refine the acquisition strategy, and to support the development of artifacts which are required to successfully achieve the ADE-2 milestone. Staff within the Acquisitions Directorate stated that they were also in the process of finalizing a life cycle cost estimate and a project plan for eHRa—documents necessary for ensuring that appropriate business decisions will be made regarding eHRa's logistics, affordability, and resources, among other things.

As of December 2017, the Coast Guard had not yet made a final determination as to which option would be chosen as the solution for the eHRa acquisition. Until a solution is chosen and successfully implemented, the Coast Guard and its thousands of members will continue to face the many challenges inherent with managing and maintaining paper health records.

Conclusions

The Coast Guard abruptly discontinued the IHiS project in 2015, citing financial, technical, schedule, and personnel risks. Coast Guard officials estimate this failed project has thus far cost the agency about $60 million. Further, this effort left the Coast Guard without any reusable system components for future EHR efforts.

The Coast Guard could not demonstrate that it had fully implemented effective management and oversight for the IHiS project prior to its discontinuance. Specifically, the Coast Guard could not fully show key project management actions were taken for IHiS, lacked governance mechanisms, and did not document lessons learned for the failed project. By not doing so, the agency reduced the probability of the project's success.

The Coast Guard's decision to revert to a predominately paper process has created a number of challenges for its many clinics and sick bays. These challenges are hindering their ability to deliver services. To help

alleviate several of these challenges, the Coast Guard's clinics and sick bays have developed alternative work-around processes. However, these alternative processes will likely not provide sustained solutions.

The Coast Guard is currently taking steps to plan for a new EHR system, but as of December 2017—over 2 years after the cancelation of the IHiS project—it had not yet selected another solution. Successfully and quickly implementing an EHR system is vital to overcoming the challenges the Coast Guard currently faces in managing paper health records. The expeditious and judicious implementation of such a system can significantly improve the quality and efficiency of care to the thousands of Coast Guard active duty and reserve members that receive health care.

Recommendations for Executive Action

We are making the following four recommendations to the Coast Guard:

The Commandant should direct the Chief Information Officer and the Chief Acquisition Officer to expeditiously and judiciously pursue the acquisition of a new EHR system. (Recommendation 1)

The Commandant should direct the Chief Information Officer and the Chief Acquisition Officer to ensure established processes required for the future acquisition or development of an EHR are effectively implemented and adequately documented. (Recommendation 2)

The Commandant should direct the Chief Information Officer and the Chief Acquisition Officer to establish and fully implement project governance boards for the future EHR effort that include the Chief Information Officer. (Recommendation 3)

The Commandant should direct the Chief Information Officer and the Chief Acquisition Officer to document any lessons learned from the discontinued IHiS project, share them with the new project management team, and ensure lessons learned are utilized for the future EHR effort. (Recommendation 4)

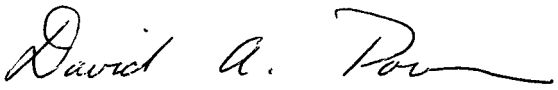
Agency Comments and Our Evaluation

The Department of Homeland Security provided written comments on a draft of this report. In its comments (reprinted in appendix VI), the department concurred with our four recommendations and identified actions being taken or planned to implement them. Among these actions, the department stated that it is judiciously pursuing an EHR solution, called eHRa, through its acquisition process, which is currently in the analyze/select phase of the NMAP process. The department also stated that a contract award for eHRa is planned for later this fiscal year. In addition, the department stated that it established a designated acquisition program with a dedicated program management office team and oversight council for EHR activities, and that the EOC monitors eHRa's progress through the acquisition process. The department further added that governance boards for eHRa have been established that include the CIO as required by the NMAP manual. Finally, the department said that it plans to compile lessons learned from the discontinued IHiS project by March 30, 2018.

Given the actions identified, the department requested that we consider the first three of our four recommendations to be closed. However, while the Coast Guard is taking positive steps with regard to initiating the eHRa program, the department noted that key decisions related to analyzing, selecting, and acquiring the new system remain to be made. Further, the Coast Guard has not yet awarded a contract for an EHR solution and is not planning to do so until later this fiscal year. Thus, the extent to which it establishes and effectively implements processes and governance boards throughout the project, and expeditiously and judiciously pursues the acquisition of the new system, remain to be seen. Accordingly, we will not yet close any of the recommendations. The department also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Homeland Security, the Commandant of the Coast Guard, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9286 or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.



David A. Powner
Director, Information Technology Management Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of this study were to (1) describe what led the United States Coast Guard (Coast Guard) to the decision to terminate further Integrated Health Information System (IHiS) development, and how much was spent on the project; (2) evaluate the Coast Guard's management and oversight actions for the discontinued electronic health records (EHR) modernization project and what, if any, lessons learned were identified; (3) describe the Coast Guard's current process for managing health records and the challenges, if any, it is encountering; and (4) determine the Coast Guard's plans for effectively implementing a new EHR system and the current status of its efforts.

To address the first objective, we reviewed relevant IHiS project documentation, such as key contracts, the project plan, presentations by the project management team, and IHiS-related memorandums. We also reviewed project expenditures documentation developed by the Deputy Commandant for Mission Support and the Acquisitions Directorate. We supplemented our review with interviews of agency officials within the Health Safety and Work-Life (HSWL) Directorate, Office of Budget and Programs, Office of Resource Management, Office of Contract Operations, and the Office of Acquisition Support, as well as six key contractors.

To address the second objective, we reviewed relevant policies and guidance, such as the Coast Guard's *Command, Control, Communications, Computers and Information Technology (C4&IT) System Development Life Cycle (SDLC) Policy*[1] *and the SDLC Practice Manual*[2] intended to guide the management and oversight of development and acquisition projects at the Coast Guard. We evaluated available IHiS project management documentation, such as project plans, the project's schedule, decision memorandums, charters for IHiS governing bodies, and Executive Oversight Council (EOC) meeting minutes, which demonstrated actions taken by project management staff during the IHiS project, and assessed them against selected practices identified in the Coast Guard's *SDLC Practice Manual*. The practices we selected are fundamental to effective information technology (IT)

[1]Coast Guard, *Command, Control, Communications, Computers and Information Technology (C4&IT) System Development Life Cycle (SDLC) Policy, Commandant Instruction 5230.66A* (Washington, D.C.: Dec. 11, 2009).

[2]Coast Guard, *U.S. Coast Guard Systems Development Life Cycle (SDLC) Practice Manual, Revision 1.0* (Washington, D.C.: Dec. 11, 2009); and *U.S. Coast Guard SDLC Practice Manual, SDLC Product #107 Revision 4.0* (Washington, D.C.: Nov. 30, 2011).

management and oversight. These included practices for conceptual planning, planning and requirements, design, and development and testing.[3] We selected the practices from each applicable phase that had an associated artifact or called for the agency to take specific action(s) that we were able to validate through evidentiary review. If an artifact was applicable to multiple practices in multiple phases of the SDLC, we evaluated the artifact in only one phase and one practice.

We also interviewed agency officials from Coast Guard offices such as the HSWL Directorate, Office of Budget and Programs, and Office of Resource Management regarding their role in managing and overseeing the IHiS project. In addition, we interviewed or received written responses from knowledgeable representatives for six key contractors tasked with providing the ambulatory care system and patient portal, safety data management and user credentialing system, software, and engineering and acquisition technical assistance. These interviews focused on the contractor's role in the IHiS project, any issues they experienced, and the status of the services they were providing at the time of cancelation. Lastly, we interviewed Coast Guard officials within the HSWL and Acquisition Directorates to determine whether lessons learned were obtained and documented to inform future decisions for the new EHR project.

Our methodology to determine the extent to which the Coast Guard demonstrated the completion of the selected SDLC phase practices included three levels of assessment: (1) the Coast Guard provided documentation that demonstrated that the IHiS project satisfied all of the elements of the required SDLC project management practice; (2) the Coast Guard provided documentation that demonstrated that the IHiS project partially satisfied some but not all elements of the required SDLC project management practice; and (3) the Coast Guard could not provide documentation that demonstrated that the IHiS project satisfied any of the elements of the required SDLC project management practice.

To address the third objective, we reviewed Coast Guard medical records management documentation, such as medical manuals, workflow procedures, and standard operating policies and procedures for clinics and sick bays. We also administered a survey via e-mail questionnaire to

[3]Practices from the remaining three SDLC phases—Implementation, Operations and Maintenance, and Disposition—were not applicable to the project as it was canceled prior to system implementation.

all of the 12 HSWL Regional Managers[4] and a web-based survey to all of the 166 clinic and sick bay administrators. The survey to Regional Managers included questions on whether the clinics and sick bays in their region faced challenges in managing health records without an EHR system in place and whether all the records from decommissioned EHR systems had been included in the paper records. The survey to clinic and sick bay administrators included questions on the challenges reported by Regional Managers and the mitigation strategies, if any, employed for the challenges identified. Before administering the surveys we pretested them by interviewing 1 Regional Manager and 5 clinic and sick bay administrators[5] to ensure that our survey questions and skip pattern were clear and logical and that respondents could answer the questions without undue burden.

We administered the survey to the 12 Regional Managers from March 2017 to April 2017; therefore, the corresponding responses reflect information and views as of that time period. We received 12 responses, for a 100 percent response rate. We administered the survey to the clinic and sick bay administrators from April 2017 to August 2017; therefore, the corresponding responses reflect information and views as of that time period. We received 120 responses, for a 72 percent response rate.

To address the fourth objective, we identified the process through which the Coast Guard is managing its acquisition of its new system, the *Non-Major Acquisition Process (NMAP) Manual.*[6] We then obtained planning documentation, such as relevant memorandums that described the Coast Guard's need for an EHR, the Coast Guard's request for information to assess industry capabilities for market research purposes, and a capabilities analysis study plan to identify gaps in the Coast Guard's EHR capabilities. We also reviewed a capabilities analysis report which details required capabilities for improving patient care, and an alternatives analysis report which details solutions the Coast Guard should consider based on performance, risk, cost, and schedule. We assessed these

[4]HSWL regions included: Boston, Academy, National Capital, Cape May, Portsmouth, Miami Beach, New Orleans, Cleveland, Alameda, Seattle, Honolulu, and Kodiak.

[5]We conducted pretests with the National Capital Regional Manager, Air Station Atlantic City Clinic Administrator, Base Boston Clinic Administrator, Sector Delaware Bay Sick Bay Administrator, Sector Ohio Valley Sick Bay Administrator, and Air Station Savannah Clinic Administrator.

[6]Coast Guard, *COMDTINST M5000.11B: Non-Major Acquisition Process (NMAP) Manual*, (Washington, D.C.: Dec. 31, 2012).

documentation against requirements identified in the NMAP, specifically within the first phase of the acquisition process. We also interviewed officials within the Acquisition Directorate to determine the status of the efforts to acquire or develop a new EHR system.

We conducted this performance audit from October 2016 to January 2018 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 II: Summary of the Coast Guard's SDLC Phases and Selected Project Management Practices

The Coast Guard implemented the Systems Development Life Cycle (SDLC) process for non-major information technology (IT) acquisitions in 2004 to help ensure IT projects are managed effectively and meet user needs. The process, as described in the Coast Guard's *SDLC Practice Manual*, consists of seven phases and related practices[1]—30 of which we selected for evaluation for the initial four SDLC phases of Integrated Health Information System (IHiS).[2] The following is a summary of each SDLC phase and a description of the project management practices we selected for review:

Phase 1: Conceptual Planning

This phase is the first step of the development or significant enhancement process. During this phase, high-level business needs are identified, a concept for fulfilling the business needs is proposed and validated, and resources are committed. Activities (or practices) we selected for review in this phase include formalizing SDLC role designations, such as the project manager, asset manager, and sponsor;[3] developing the initial business case with information regarding the background, system justification, and project risk management, among other things; validating alignment with the enterprise architecture; identifying the funding source and providing a rough order of magnitude cost estimates as part of developing the acquisition strategy; designating the system as a Command, Control, Communications, Computers, and Information Technology (C4&IT) system; and obtaining approval to exit the conceptual planning phase.

[1]Coast Guard, *U.S. Coast Guard Systems Development Life Cycle (SDLC) Practice Manual, Revision 1.0* (Washington, D.C.: Dec. 11, 2009); *U.S. Coast Guard SDLC Practice Manual, SDLC Product #107 Revision 4.0* (Washington, D.C.: Nov. 30, 2011).

[2]The remaining three phases—Implementation, Operations and Maintenance, and Disposition—were not applicable since the IHiS project was canceled prior to system implementation.

[3]The project manager is to be designated by the Chief Information Officer (CIO) with responsibility and authority to accomplish project cost, schedule, and performance objectives for developing, producing, and deploying an asset within established business and technical policy and standards guidelines. The asset manager, also to be designated by the CIO, is responsible for guiding, overseeing, and monitoring execution of the SDLC for all assigned C4&IT assets. The sponsor validates the business need for the system. The sponsor(s) role is fulfilled by the Coast Guard organization that defines and articulates organizational goals, validates requirements, and acquires the necessary resources for the system. The sponsor is the high level entity that can speak to organizational needs and is aware of the relationships of developing this system to other Coast Guard initiatives.

Phase 2: Planning and Requirements

This phase begins after the project has been defined and appropriate resources have been committed. During this phase, business requirements are collected, defined, and validated. More specifically, as part of the phase practices we selected for review, the SDLC tailoring plan[4] is completed; and initial life cycle management plans for project management, risk management, integrated logistics support,[5] training, and information assurance[6] are developed. In addition, a cost benefit analysis is conducted; functional requirements are documented; external mandates are reviewed; the system development agent and system support agent are designated;[7] and approval to exit the planning and requirements phase is obtained.

Phase 3: Design

During this phase, business requirements are translated into system requirements to develop the detailed system design. Selected practices for this phase include developing the detailed system design to specify the operating system, architecture components, timing and sizing, and interfaces, among other things; developing the operational analysis plan to document system performance measures, system operating measures that address reliability, maintainability, availability, training, and user

[4]A tailoring plan provides a clear and concise listing of SDLC process requirements throughout the entire system lifecycle, and facilitates the documentation of calculated deviations from standard SDLC activities, products, roles, and responsibilities from the outset of the project.

[5]The integrated logistics support plan is a logistic document that begins the life cycle parts support for approved equipment. It also indicates the type, quantity, and characteristics of the equipment installed, and includes plans for configuration management, data management, records management, and quality assurance.

[6]The information assurance plan includes information security controls that are intended to ensure information integrity, authentication, confidentiality, and non-repudiation.

[7]A system development agent is an individual, unit, firm, agency, or organization that performs, or has the responsibility for, the design, development, implementation, and support of C4&IT systems, as well as acquisition of products or services. Similarly, a system support agent performs, or has the responsibility for, the maintenance and support of C4&IT systems as they are used in the field and within Coast Guard programs. The system support agent participates in all aspects of the C4&IT SDLC. Together with the system development agent, the system support agent ensures that C4&IT systems are built to improve mission performance and sustain availability with the lowest total ownership cost, taking into account the supportability requirements and costs associated with sustaining enterprise systems.

satisfaction; and system support measures containing the level of effort needed to support the system; conducting review sessions with the user community to ensure that the system design sufficiently met all functional requirements; developing contingency and disaster recovery plans; completing the privacy impact analysis; documenting the test and evaluation master plan with the scope, content, methodology, sequence, management of, and responsibilities for test activities; testing the system design according to the operational test and evaluation plan and capturing design test results in the test and evaluation master plan; and obtaining approval to exit the design phase.

Phase 4: Development and Testing

The system is developed or acquired based on detailed system design specifications and validated through a variety of tests during this phase. The objective is to ensure that the system functions as expected and that sponsor and user requirements are satisfied. More specifically, as part of the phase practices that we selected, system testing is conducted; system documentation, such as system manuals, user manuals, and diagrams of the system is developed; an implementation plan[8] is developed; and an authority to operate[9] is obtained.

Phase 5: Implementation

During this phase, the system is placed in the production environment and system users are trained. It also includes efforts required to implement the system and resolve problems identified during the system's transition from development to deployment. We did not select practices to evaluate in this phase since the system was discontinued before implementation.

[8]The implementation plan is an established plan for the installation and deployment of systems. This plan contains expected dates, resources required, interfaces and relationship between events, and responsibilities for accomplishing the following events: installation of equipment; loading of software and firmware; when, where, what, and to whom equipment and documentation will be sent; quantities; and required delivery dates.

[9]The National Institute of Standards and Technology Special Publication 800-37 defines the authority to operate as the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls.

Phase 6: Operations and Maintenance

The system becomes operational during this phase, and its main purpose is to ensure that the system continues to perform according to specifications. In addition, routine hardware and software maintenance and upgrades are performed to ensure effective system operations; user training continues as needed; and additional user support is provided to help resolve reported problems. We did not select practices to evaluate in this phase since the system was discontinued before implementation.

Phase 7: Disposition

This phase represents the end of the system's life cycle. It provides for the systematic termination of a system to ensure that vital information is archived. The emphasis of this phase is to ensure that the system (e.g., equipment, software, data, procedures, and documentation) is packaged and disposed of in accordance with appropriate regulations and requirements. We did not select practices to evaluate in this phase since the system was discontinued before implementation.

Appendix III: Copy of the Survey That GAO Administered to Coast Guard Health Safety and Work-Life Regional Managers

The questions we asked in our survey of the 12 Health Safety and Work-Life (HSWL) Regional Managers from March 2017 to April 2017 are shown below. For a more detailed discussion of our survey methodology see appendix I.

1. Generally, what challenges, if any, have the clinics and sickbays in your region faced with using paper health records?

   a. What specific challenges, if any, have the clinics and sickbays in your region faced after the decommissioning of the Composite Healthcare System (CHCS) in February 2016 and Provider Graphical User Interface (PGUI) in September 2015?

   b. What steps, if any, have been taken in your region to address these challenges?

   c. What steps, if any, are being planned in your region to address these challenges?

2. Prior to the decommissioning of CHCS/PGUI, did your region verify that all electronic health records were copied to paper records?
   - ☐ Yes (Complete 'a' and 'b' below)
   - ☐ No (Skip to 2.1)
   - ☐ Don't Know (Skip to 3)

   a. If yes, please describe the verification process.

   b. What date was the verification process completed?

2.1. If no, please explain why your region did not verify that all electronic health records were copied to paper records.

3. After the decommissioning of CHCS/PGUI, were any of your region's electronic health records that were previously stored in CHCS/PGUI not included in the paper records?
   - ☐ Yes (Complete 'a' below)
   - ☐ No (Skip to 4)
   - ☐ Don't Know (Skip to 4)

   a. If yes, how many electronic records were not included in the paper records?

4. Are paper records inspected for errors or missing information?
   - ☐ Yes (Complete 'a' and 'b' below)
   - ☐ No (Skip to 5)
   - ☐ Don't Know (Skip to 5)

   a. If yes, how often are paper records inspected for errors or missing information?

   b. Is there a procedure outlining how to inspect the records for errors or missing information?
      - ☐ Yes
      - ☐ No
      - ☐ Don't Know

5. What is the process, if any, for correcting errors to paper records?

6. What is the process, if any, for locating and replacing lost or damaged paper records?

7. In what month and year did you start your position as a Regional Manager?

8. What are the names of the clinics and sickbays in your region and how many patients does each location serve? Please provide contact information for an administrator for each location.

Clinic Title	Number of Patients Served	Clinical Administrator (Name)	Clinical Administrator (Email Address)

Sickbay Title	Number of Patients Served	Health Services Administrator (Name)	Health Services Administrator (Email Address)

9. If you have any additional comments related to Coast Guard's health records and health record management system please provide them here.

Source: GAO. | GAO-18-59

Appendix IV: Copy of the Survey That GAO Administered to Coast Guard Clinic and Sick Bay Administrators

The questions we asked in our survey of the 166 clinic and sick bay administrators from April 2017 to August 2017 are shown below. For a more detailed discussion of our survey methodology see appendix I.

General Information

1. Is your facility a clinic, a sick bay, or another type of facility?
   - ○ Clinic
   - ○ Sick bay
   - ○ Other type of facility

   ↻ Reset

2. What is the name of your facility?

3. How many patient records are currently managed by your office?
   - ○ 0 - 200
   - ○ 201 - 500
   - ○ 501 - 1,000
   - ○ 1,001 - 1,500
   - ○ Over 1,500

   ↻ Reset

Challenges

4. While using paper records, how challenging, if at all, have the following experiences been for you and your office staff?
For the purposes of this survey "Very challenging," means a large degree of challenge, "moderately challenging," means a small to average degree of challenge, and "not at all challenging," means it has not posed a challenge.

Click one answer in each row, and if the item was a challenge, don't know, or not applicable, please explain.

	How challenging, if at all?	If a challenge, don't know, or not applicable, please explain.
a. Incomplete records	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	
b. Missing records	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	
c. Amount of time of patient encounters	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	

	How challenging, if at all?	If a challenge, don't know, or not applicable, please explain.
d. Amount of time to schedule appointments	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	
e. Amount of time to manage records	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	
f. Availability of records	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	
g. Track medications	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	

○ Very challenging

	How challenging, if at all?	If a challenge, don't know, or not applicable, please explain.
h. Conduct consultations with other doctors	○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	

	How challenging, if at all?	If a challenge, don't know, or not applicable, please explain.
i. Send referrals	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	
j. Ability to view/print lab reports	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	
k. Order x-rays	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable ↻ Reset	

l. Combine data to understand health trends in the community

- ○ Very challenging
- ○ Moderately challenging
- ○ Not at all challenging
- ○ Don't know
- ○ Not Applicable

Reset

	How challenging, if at all?	If a challenge, don't know, or not applicable, please explain.
m. Ability to read penmanship	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable Reset	
n. Cost of maintaining records	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable Reset	
o. Security/privacy of records	○ Very challenging ○ Moderately challenging ○ Not at all challenging ○ Don't know ○ Not Applicable Reset	

p. Ability to search within	○ Very challenging ○ Moderately challenging ○ Not at all challenging	
	How challenging, if at all?	**If a challenge, don't know, or not applicable, please explain.**
records for information	○ Don't know ○ Not Applicable ↻ Reset	

5. Do you have any additional challenges with using paper records that were not provided above?
   - ○ Yes
   - ○ No

↻ Reset

Additional Steps

6. Has your office taken the following steps to address the challenges with using paper health records and if so, please explain?

	Did you take the following steps?	If yes, please explain.
a. Developed additional forms	○ Yes ○ No ○ Don't know ○ Not Applicable ↻ Reset	
b. Developed tracking methods to collect data	○ Yes ○ No ○ Don't know ○ Not Applicable ↻ Reset	
c. Developed alternate processes	○ Yes ○ No ○ Don't know ○ Not Applicable ↻ Reset	
d. Notified management of challenges	○ Yes ○ No ○ Don't know ○ Not Applicable ↻ Reset	
e. Other steps	○ Yes ○ No ○ Don't know ○ Not Applicable ↻ Reset	

Decommissioning of CHCS/PGUI

7. After the decommissioning of the Composite Healthcare System (CHCS) in February 2016 and the Provider Graphical User Interface (PGUI) in September 2015, were any electronic health records that were previously stored in CHCS/PGUI not included in the paper records?
   - ○ Yes
   - ○ No
   - ○ Don't Know

   Reset

8. Prior to the decommissioning of CHCS/PGUI, was a review conducted to verify that all electronic health records were copied to paper records?
   - ○ Yes – Review completed
   - ○ Yes – Review attempted
   - ○ No
   - ○ Don't Know

   Reset

Final Questions

9. Do you have documentation of standard operating procedures and processes for managing health records for your office?
   - ○ Yes
   - ○ No
   - ○ Don't Know

   Reset

10. If you have any additional comments related to Coast Guard's health records and health record management system, please write them in the box below.

Submit Your Final Responses to GAO

11. **Are you ready to submit your final completed survey to GAO?**

(This is equivalent to mailing a completed paper survey to us. It tells us that your answers are official and final.)

- ○ Yes, my survey is complete - *To submit your final responses, please click on "Exit and save" below"*
- ● No, my survey is not yet complete - *To save your responses for later, please click on "Exit and save" below"*

↻ Reset

You may view and print your completed survey by clicking on the Summary link in the menu to the left.

Print responses

Close window

Source: GAO. | GAO-18-59

Appendix V: Summary of the Coast Guard's Non-Major Acquisition Process Acquisition Decision Events and Phases

Coast Guard's *Non-Major Acquisition Process (NMAP) Manual*[1] defines the process for the designation, management, and oversight of non-major acquisitions. The NMAP requires formal approval reviews at three discrete knowledge points called acquisition decision events (ADE) and includes three phases to assess the readiness and maturity of the acquisition. The phases represent work that must be accomplished to demonstrate readiness to proceed to the next phase. The following is a summary of each ADE and subsequent phase within the NMAP:

- ADE-1 occurs when the Deputy Commandant for Mission Support designates the procurement as a non-major acquisition and approves the acquisition to enter the analyze/select phase. Following ADE-1 approval, the Chief Acquisition Officer or Chief Information Officer (CIO) designates a project manager. The analyze/select phase includes project management activities such as conducting market research to identify available alternatives, preparing a requirements document, developing an acquisition strategy, developing a life cycle cost estimate, and preparing a project plan.
- The primary purpose of ADE-2 is to approve the alternatives identified through market research and to assess the readiness of the acquisition for a contract award in which the acquisition moves into the obtain phase. The CIO is the decision authority and provides oversight for ADE-2. The obtain phase includes activities such as evaluating whether the proposed solution can effectively meet the functional requirements, initiating deployment planning, and conducting usability testing.
- The primary purpose of ADE-3 is to assess the readiness of the acquisition to be deployed and supported by authorizing the acquisition to enter the produce/deploy and support phase. The CIO is the decision authority and provides oversight for ADE-3. The produce/deploy and support phase includes activities such as ensuring the delivered product meets cost, schedule, and performance baselines as described within the project plan, as well as executing production contracts.

[1]Coast Guard, *Non-Major Acquisition Process (NMAP) Manual*, COMDTINST M5000.11B (Washington, D.C.: Dec. 31, 2012). As of August 2017, the Coast Guard was in the process of updating the NMAP.

VI: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

December 28, 2017

David A. Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report: GAO-18-59, "COAST GUARD HEALTH RECORDS: Timely Acquisition of New System is Critical to Overcoming Challenges with Paper Process"

Dear Mr. Powner:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition that while the Coast Guard is currently using a predominantly paper process to document health care services for its military members, it has (1) developed alternative work-around processes to help alleviate challenges associated with this process, and (2) initiated the process for acquiring a new electronic health record (EHR) system to replace the current paper-based process. The Coast Guard is committed to efficiently providing its members the best healthcare possible.

The draft report contained four recommendations with which the Department concurs. Attached find our detailed response to each recommendation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

Attachment: Management Response to Recommendations Contained in GAO-18-59

GAO recommended that the Commandant of the Coast Guard:

Recommendation 1: Direct the Chief Information Officer [CIO] and the Chief Acquisition Officer [CAO] to expeditiously and judiciously pursue the acquisition of a new EHR system.

Response: Concur. The Coast Guard is judiciously pursing an electronic health record solution through its acquisition process. To that end, the Coast Guard initiated the Electronic Health Record Acquisition (eHRa) program, which is currently in the Analyze and Select Phase. During this phase the foundation is established that prepares an acquisition program for contract award(s), which is made in the Obtain Phase. The eHRa's Acquisition Decision Event (ADE-2) to exit the Analyze/Select phase and enter the Obtain Phase is planned for later this fiscal year. We request that GAO consider this recommendation closed as implemented.

Recommendation 2: Direct the CIO and the CAO to ensure established processes required for the future acquisition or development of an EHR are effectively implemented and adequately documented.

Response: Concur. By employing its acquisition process and governance, in accordance with the Coast Guard's Non-Major Acquisition Process (NMAP) manual, the Coast Guard– per direction from the Vice Commandant of the Coast Guard and the Deputy Commandant for Mission Support– has a designated acquisition program established with a dedicated program management office team for EHR activities. Each designated acquisition program has an oversight council. The Executive Oversight Council (EOC) monitors eHRa's progress through the acquisition process. Members of the EOC include the CAO (chair), and Health, Safety and Work-Life (HSWL) (sponsor) among other senior leaders. On February 2, 2016, HSWL requested that the EOC recommend approval for an EHR acquisition program. Subsequently, on February 13, 2016, DCMS granted approval to (a) designate and establish the eHRa program, and (b) for eHRa to enter the Analyze/Select phase of the acquisition process. In accordance with the NMAP, eHRA has various topic-specific integrated product teams (IPTs) to address the range of issues associated with the Analyze/Select phase activities. We request that GAO consider this recommendation closed as implemented.

Recommendation 3: Direct the CIO and the CAO establish and fully implement project governance boards for the future EHR effort that include the CIO.

Response: Concur. The Coast Guard's NMAP manual, established governance boards for eHRa are: the EOC that includes both the CAO and CIO as members, and IPTs that have CAO and CIO representatives. We request that GAO consider this recommendation closed as implemented.

2

Recommendation 4: Direct the CIO and the CAO to document any lessons learned from the discontinued IHiS project, share them with the new project management team, and ensure lessons learned are utilized for the future EHR effort.

Response: Concur. The Coast Guard's Deputy Commandant for Mission Support will compile cross directorates' lessons learned of the discontinued IHiS project that resided in Health, Safety and Work-Life at the time of the cancellation. Consolidation of lessons learned will include assistance from the CIO and CAO as well as factor in the previous audit report, DHS OIG-18-15, "Coast Guard IT Investment Risk Failure without Required Oversight" and this current review by GAO. The documented lessons will be provided to new EHR acquisition program management team and it's Executive Oversight Council. Estimated Completion Date: March 30, 2018.

3

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

David Powner, (202) 512-9286 or pownerd@gao.gov

Staff Acknowledgments

In addition to the contact named above, key contributors to this report were Nicole Jarvis (Assistant Director), Ashfaq Huda (Analyst in Charge), Chris Businsky, Juana Collymore, Sharhonda Deloach, Rebecca Eyler, Andrea Harvey, Gina Hoover, Jason Lee, Rob Letzler, Monica Perez-Nelson, Kelly Rubin, and Andrew Stavisky.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.