


GETTING READY TO GET READY GUIDE

Indian Health Service
Health Information Technology
Modernization Program

CONTENTS

Getting Ready to Get Ready: Recommended Actions

Complete a **Statement of Interest (SOI)**.

Fill all **key staffing positions** required to support daily operations.

Ensure all **contracts and agreements** are up to date.

Develop or update your **Continuity of Operations Plan (COOP)** or **Downtime Procedure**.

Identify **ports, protocols, and interfaces of all biomedical devices** at your facility.

Update Resource and Patient Management System (RPMS) to the **most recent, certified version**.

OR

Ensure commercial EHR meets the **Certified Health Information Technology (CHIT), 2015 Edition CURES requirements**.

Ensure **local area network** (**LAN**) and **wide area network** (**WAN**) connectivity are available and function at a high capacity.

Keep **Revenue Cycle operations** up to date based on the guidelines provided through go-live.

Review **NIST Federal Information Security Management Act (FISMA)** for policies and guidelines concerning ePHI and resolve any discrepancies or issues.

Conduct a **National Institute of Science and Technology (NIST) Framework Analysis** for Security Hardening audits and review.

Stay connected and engaged with the **IHS Health IT Modernization Program's website, blog, and social media**, and attend events including **TC/UCs** and **summits**.

PURPOSE

The Indian Health Service (IHS) Health Information Technology (IT) Modernization Program will work with tribal and urban partners to build an enterprise health IT solution that supports delivery of high-quality health care across Indian Country. The IHS selected and purchased an enterprise electronic health record (EHR) solution to increase interoperability and improve software functionality in the delivery of care. Interoperability allows programs to share information across IHS/tribal/urban (I/T/U) locations and with referral network partners in the private sector and government health care spaces.

The Getting Ready to Get Ready Guide provides I/T/U sites with tasks that need to be completed as the initial step of the implementation process. I/T/U sites will be selected for inclusion in an implementation cohort — a group of sites that go through implementation and go-live simultaneously — in part based on their completion of the tasks included in this guide. Completion of these tasks does not guarantee immediate inclusion in a cohort; however, completion moves a site closer to a state of implementation readiness. This guide includes tasks to be completed in the following categories:

- Technical
- Staffing
- Security
- Business processes

This guide is for informational purposes only and is designed to help sites as they prepare to engage in the Modernization Program. The Implementation and Deployment team within the IHS contacts sites at the appropriate time to assist them with a deeper dive into next steps for enterprise EHR solution implementation.

I. STATEMENT OF INTEREST

This section applies to Title 1 and Title 5 Tribes and urban Indian organizations who are interested in implementing the new enterprise EHR solution.

Complete a Statement of Interest (SOI).

Why this is important:

One of the central principles of the Indian Health Service (IHS) Health Information Technology (IT) Modernization Program is to build and operate the enterprise electronic health record (EHR) solution with our partners, not for them. The IHS invites sites that are considering the new enterprise EHR solution as a viable option to complete the Statement of Interest (SOI) to indicate their interest in participating in shared enterprise solution planning.

This non-binding SOI helps the IHS understand which sites are interested in becoming part of the new enterprise EHR solution partnership and asks for limited details about those organizations, such as facility size, current EHR utilization, and point(s) of contact.

How to complete:

Complete the Statement of Interest (SOI):
Statement of Interest Participation in IHS Multi-Tenant Enterprise EHR.

Submit the SOI by email to modernization@ihs.gov. There is no deadline for submitting the form and federal sites are not required to complete the SOI document. The IHS IT Modernization Program Management Office reaches out to organizations that provide the SOI to learn more about their facilities, services, and staffing that may need support from the new enterprise EHR solution. Subject matter experts from interested organizations can provide individual input in their areas of expertise regarding the configurations and workflows that the new enterprise EHR solution should provide.

Are you a leader within a tribal/urban Indian organization?

Fill out the Statement of Interest and email it to **modernization@ihs.gov**

**There is no deadline for submission*

II. KEY STAFFING POSITIONS

Fill all key staffing positions required to support daily operations.

Why this is important:

Filling key staffing positions helps the organization have the stability and support needed to successfully implement the new enterprise electronic health record (EHR) system. Key staffing positions may differ for each site.

How to complete:

Review your site's staffing model and make note of all vacant positions. Prioritize filling the positions that are most impactful in supporting daily operations of the site. Key clinical and ancillary staff positions include, but are not limited to, providers, clinical applications coordinators and informaticists, revenue cycle personnel, PRC personnel, nurses, radiology technicians, lab personnel, pharmacists and pharmacy technicians, operational leadership, and IT support staff

III. LEGACY ELECTRONIC HEALTH RECORD SYSTEMS

If your site uses the Resource and Patient Management System (RPMS), update it to the most recent, certified version.

If your site uses a commercial electronic health record, ensure it is updated to meet the Certified Health Information Technology (CHIT), 2015 Edition CURES requirements.

Why this is important:

An updated infrastructure helps guarantee your data remains secure and your systems run as smoothly as possible. By updating your legacy EHR to the latest version, the fields and data coming from your system better match the information going into the new enterprise EHR solution, thereby giving you a cleaner transition.

How to complete:

If you use RPMS, you can view the latest IHS certified applications here.

If you use a commercial EHR, you can view the most recent certified version of your software from the ONC Certified Product List website.

IV. CONTINUITY OF OPERATIONS PLAN OR DOWNTIME PROCEDURE

Develop or update your Continuity of Operations Plan (COOP) or Downtime Procedure.

Why this is important:

Even the most efficient technology has occasional downtime when the system or the infrastructure does not work. Sometimes these outages are planned, usually for upgrades or maintenance, and sometimes they are not planned. Regardless of the reason for the outage, patient care must continue. A COOP (also known as a Downtime Procedure) defines what to do and how to document patient care during the outage. Comprehensive COOPs address all aspects of downtime, including background systems that update regularly while the system is functioning properly that offer access to schedules and limited patient data during a downtime, where to find paper forms for patient care documentation, and how and when documentation created during the downtime is entered into the EHR once systems are back up and running.

How to complete:

The IHS has already implemented a Continuity of Operations Planning Program. Sites without a COOP in place should refer to the IHS's Continuity of Operations Planning Program when developing their plan. Sites with an existing COOP should refer to the Continuity of Operations Planning Program to validate the plan for adequacy and completeness.

Visit IHS Continuity of Operations Planning Program for more guidance concerning how to develop a comprehensive COOP.

V. NETWORK CONNECTIVITY AND USAGE

Assess local area network (LAN) and wide area network (WAN) connectivity to ensure it is available and functions at a high capacity.

Why this is important:

The new enterprise EHR solution is cloud-based. To work appropriately and give end users the experience it is designed to deliver, network connectivity must be robust and function at a high capacity everywhere documentation is created or reviewed.

Reviewing the activity and status of your facility's network allows you to identify and address potential issues, such as network congestion, security vulnerabilities, or hardware failures. Monitoring network activity provides insights into usage patterns, helping optimize performance and allocate resources effectively. Regular reviews also enable proactive measures, enhancing overall reliability and minimizing downtime. Additionally, staying abreast of network status ensures compliance with security protocols, protecting sensitive data and preventing unauthorized access. Overall, this practice is essential for maintaining a robust, efficient, and secure network infrastructure in your facility.

How to complete:

Complete the following to verify strong network connectivity throughout a facility and guarantee a robust and reliable network infrastructure:

- Conduct a comprehensive site survey to identify potential areas with weak signal strength or interference.
- Use network monitoring tools to assess the performance of routers, switches, and access points, checking for any bottlenecks or points of failure.
- Perform thorough testing of wireless connectivity in various locations within the facility, taking note of signal strength, latency, and packet loss. Complete this activity with devices that will be used on the network for EHR-related functions.
- Verify that all network devices are properly configured and updated with the latest firmware and drivers.
- Ensure sufficient bandwidth to support the anticipated network traffic.
- Conduct periodic security audits to safeguard against unauthorized access and potential vulnerabilities.
- Establish redundancy and failover mechanisms to mitigate the impact of any unforeseen network issues.
- Regularly reassess and optimize the network configuration based on the evolving needs of the facility.
- IHS Network Operations and Support Center (NOSC) personnel should have up to date network diagrams for the Federal facilities and local network staff should have diagrams for tribal and urban locations. If diagrams cannot be located, new architecture diagrams should be created with the help of network staff or the IHS NOSC.
- If you are an IHS facility, from within the IHS network, use this link to access NOSC and check your network: https://nosc.ihs.gov/index.php?title=Main_Page.
- If you are a tribal or urban Indian facility, the IHS NOSC may be able to provide information pertaining to your location. If this is not available, local onsite network personnel need to conduct uptime reports or similar data gathering tasks to determine the activity on and status of your local network.

VI. REVENUE CYCLE OPERATIONS

Revenue Cycle operations should be up to date based on the guidelines below and remain up to date through go-live activities.

- Review/approve claims within five days and clear backlog of unbilled claims.
- Paper or electronic claims that go to the payer must be printed or exported within one to two days.
- All exports to your site's financial system have been completed within five days.
- All payments received by the facility are batched no later than five days from receipt.
- Payment posting should be completed within 30 days.
- Open canceled bills must be cleared.
- For federal sites: Reconciliation to the Unified Financial Management System (UFMS) must be current within 30 days.

It is important for sites to follow their third-party revenue policy.

Why this is important:

Any coding, billing, and claims created in a legacy EHR must be completed in the legacy EHR. The deeper the backlogs are, the harder they are to complete, requiring the site to work in a hybrid environment running two separate EHR billing systems for a longer period. This hybrid operation increases the possibility of errors in billing, which can negatively affect site revenue and the patient experience.
Up-to-date Revenue Cycle operations also provide a more complete picture of an organization's financial health, which may impact the success of its implementation.

How to complete:

I**HS Facilities:** Reach out to your IHS RPMS support team for assistance.

Non-IHS Facilities: Work with your Revenue Cycle manager(s) to determine how revenue cycle operations can be completed for your EHR.

VII. BIOMEDICAL DEVICES

Identify ports, protocols, and interfaces of all biomedical devices at your facility.

Why this is important:

This information is vital to the integration and interoperability of the new EHR.

How to complete:

Compiling a complete asset inventory of biomedical devices is a prerequisite for an effective assessment of infrastructure visibility. The inventory should contain details of each device, such as make, model, age, patch history, and software version. For completeness, the inventory should include network-attached and non-network-attached devices. All the information should be managed in a configuration management database (CMDB). Biomedical devices should be classified properly to guarantee accurate information.

Asset detection for network-attached devices requires scanner tools with capabilities to retrieve inventory information. The scanner conducts a thorough scan of the ports, protocols, and interfaces, which can determine discovery of endpoints. The scanner probes for specific protocols and versions such as Hypertext Transfer Protocol (HTTP), Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Shell protocol (SSH), and Simple Mail Transfer Protocol (SMTP). Network scanning is an ongoing task that results in a complete visibility of endpoints. Biomedical device information should be kept up to date to ensure compliance.

VIII. CONTRACTS AND AGREEMENTS

Ensure all contracts and agreements are up to date.

Why this is important:

Contracts and agreements that need to be reviewed for accuracy and currency include any Memoranda of Understanding (MOU), Memoranda of Agreement (MOA) , Security Agreement Summaries (SAS), and third-party license agreements including, but not limited to, software licenses and biomedical device maintenance contracts. If your site is involved in clinical trials or research studies, review the agreements for those activities. If changes are needed due to implementing a new EHR solution, begin that process.

The agreements are an IHS security requirement, which must be tracked and reviewed periodically. They ensure all affected parties understand their technical and data roles and responsibilities for the partnership between the IHS and the site. For more information about data sharing and management, review the Data Management Strategy.

One of the implementation planning process steps calls for an analysis of which contracts/agreements are no longer needed in the new environment, those that should continue with some modification, and those that should continue as is. Maintaining a comprehensive list will assist in that process.

How to complete:

The organization should:

1. Identify any services they currently contract for, including but not limited to:
    a. Radiology services
    b. Lab services
    c. Biomedical lease/maintenance agreements
    d. Pharmacy automation lease/maintenance agreements
    e. Operating systems
    f. Data sharing agreements (i.e., Registries, Health Information Exchanges (HIEs), Telecommunication Engineering Centers (TECs) Medical Devices).
2. Prepare documentation on the contract details such as renewal periods, contract/agreement management lead, any specialized reporting needed to support the contract/agreement, etc.

IX. NETWORK SECURITY AUDITS AND REVIEWS

Conduct a National Institute of Science and Technology (NIST) Framework Analysis for Security Hardening audit and review.

Why this is important:

Network Security audits and reviews are essential for the IHS infrastructure to be secure, compliant, and resilient against cyber-attacks. Maintaining a consistent hardening system is vital in reducing risk associated with network traffic manipulation, data breaches, and unauthorized access. Following the NIST Framework consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. These functions ensure a successful and holistic security program.

Security Hardening is a continuous process of locking down devices and systems to eliminate and mitigate vulnerabilities. These vulnerabilities can be flaws in the software and weaknesses which may occur in the implementation, design, configuration, or system administration. Auditing and reviewing network security secures the communication infrastructure for multiple systems. Ongoing assessments and periodic follow up confirm alignment with the hardening baseline. Trust, but verify, information security and risk management.

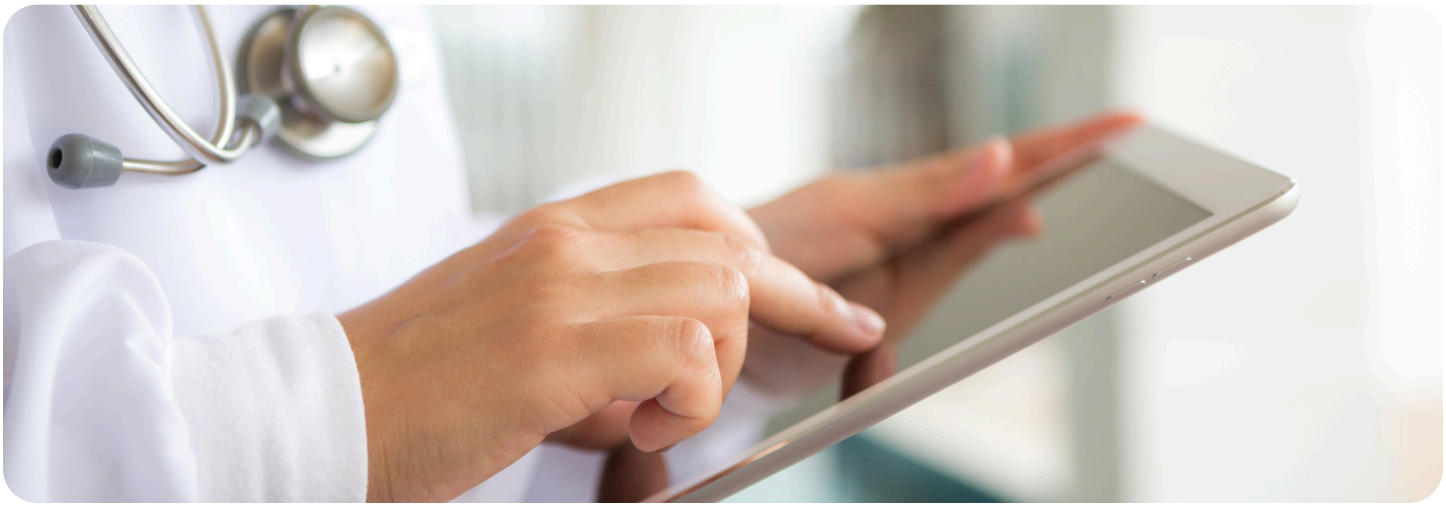
How to complete:

Current State: Identify priorities, determine compliance requirements, review existing policies, and identify vulnerabilities and risk events.

Assessment: Identify threats, review vulnerabilities, define the probability and likelihood, categorize identified risks, and create a risk heat map.

Target State: Identify mitigation approaches, translate the mitigation into desired outcomes, define goals for desired outcomes, and review and outline security priorities.

Roadmap: Quantify and score the current state, establish a budget and identify resources, define targets within the budget, and share results with stakeholders.



X. POLICIES AND GUIDELINES FOR ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)

Review NIST Federal Information Security Management Act (FISMA) for policies and guidelines concerning ePHI and resolve any discrepancies or issues.

Why this is important:

The IHS scrutinizes cybersecurity hardening, however, vulnerabilities and cyber threats are often most overlooked from the local site or area regions. NIST has created a framework to assist with hardening improvements for the local sites to mitigate threat risks.

How to complete:

To review this framework, visit https://healthitsecurity.com/features/breaking-down-the-nist-cybersecurity-framework-how-it-applies-to-healthcare. Address any discrepancies and document the findings.

XI. STAY CONNECTED

Regularly review the IHS Health IT Modernization Program website, blog, and social media pages. Attend Tribal Consultation and Urban Confer (TC/UC) events when appropriate, and join the Modernization listserv to receive email updates.

Why this is important:

Collaboration between the IHS and our tribal and urban partners is crucial for the success of the Modernization Program. There are various upcoming events and opportunities to partner with DHITMO (Division of Health Information Technology Modernization and Operations). To stay connected, please visit the Health IT Modernization Program website, blog, and social media sites. The IHS also uses a Modernization listserv to announce updates and opportunities to engage in Program activities. Please check these resources regularly for updates and announcements.

The DHITMO team's commitment to the IHS shared goals and efforts have been instrumental in driving the Health IT Modernization Program.

Resources:

- Visit the website for more information about the IHS Health IT Modernization Program
- Visit the events page on the IHS website for details on upcoming engagements
- Find the 2024 Tribal Consultation and Urban Confer (TC/UC) event schedule detailed in the January 2024 Dear Tribal Leader Letter (DTLL)
- Sign up to receive Director Tso's Bi-Weekly Updates for tribal and urban Indian leaders
- Sign up to receive Health IT Modernization Program email updates through the listserv
- Read IHS Blog posts on modernization
- Follow IHS on Facebook, LinkedIn, and X (formerly known as Twitter) to stay up to date on events, collaboration opportunities, and general Program updates

GETTING READY TO GET READY: RECOMMENDED ACTIONS

Complete a **Statement of Interest (SOI)**

Fill all **key staffing positions** required to support daily operations

Ensure all **contracts and agreements** are up to date

Develop or update your **Continuity of Operations Plan (COOP)** or **Downtime Procedure**

Identify **ports, protocols, and interfaces of all biomedical devices** at your facility

Update Resource and Patient Management System (RPMS) to the **most recent, certified version**

OR

Ensure commercial EHR meets the **Certified Health Information Technology (CHIT), 2015 Edition CURES requirements**

Ensure **local area network (LAN)** and **wide area network (WAN)** connectivity are available and function at a high capacity

Keep **Revenue Cycle operations** up to date based on the guidelines provided through go-live

Review **NIST Federal Information Security Management Act (FISMA)** for policies and guidelines concerning ePHI and resolve any discrepancies or issues

Conduct a **National Institute of Science and Technology (NIST) Framework Analysis** for Security Hardening audits and review

Stay connected and engaged with the **IHS Health IT Modernization Program's website, blog, and social media**, and attend events including **TC/UCs** and **summits**

CONNECT WITH US!

Facebook

LinkedIn

X (formerly Twitter)