



# Readiness Guide for PATH EHR

**Indian Health Service**  
Health Information Technology  
Modernization Program



- OVERVIEW ..... 2**
- PURPOSE ..... 2**
- I. ORGANIZATIONAL READINESS ..... 4**
  - Facility and Staffing Culture ..... 4
  - Governance ..... 7
- II. OPERATIONAL READINESS ..... 8**
  - PATH EHR User Access ..... 8
  - Revenue Cycle Operations ..... 9
  - Data Migration Preparedness ..... 10
  - Clinical Data Clean Up ..... 11
  - Clinical and Administrative Workflows Review ..... 11
- III. TECHNICAL READINESS ..... 12**
  - Identify Service Lines ..... 12
  - Devices and Interfaces ..... 13
  - Contracts, Agreements, and Licenses ..... 14
  - Planned Upgrades, Implementations, and Renovations ..... 16
  - Network Infrastructure of Legacy Electronic Health Records ..... 17
  - Network Connectivity and Usage ..... 18
  - Network Security Audits and Reviews ..... 19
  - Network Policies and Guidelines for Electronic Protected Health Information (ePHI) ..... 21
  - Stay Connected ..... 23
- GLOSSARY ..... 24**
- APPENDIX ..... 26**

## OVERVIEW

The Indian Health Service (IHS), in collaboration with tribal and urban Indian organization partners, is advancing a historic modernization initiative to replace the Resource and Patient Management System (RPMS) with the new PATH Electronic Health Record (EHR) platform. This modernization represents a transformative step in improving patient safety, data integrity, and care coordination across Indian Country. This new EHR platform will also provide increased interoperability, allowing information to be shared across IHS, tribal and urban Indian organizations (I/T/U) locations as well as with referral network partners in the private sector and other government healthcare spaces to ensure the delivery of high-quality healthcare.

I/T/U partners have used RPMS and other commercial EHRs for more than four decades. However, the decentralized RPMS architecture, extensive local customization, and lack of interoperability have limited the scalability and integration capabilities with national health systems. The PATH EHR initiative will promote interoperability, unify clinical, administrative, and operational functions within a modern, centralized, cloud-based enterprise solution.

This modernization effort represents more than just IT implementation. The implementation and deployment of PATH EHR is an organizational transformation that requires commitment from leaders and staff to support and nurture this important change. The Readiness Guide is divided into three readiness pillars: Organizational Readiness, Operational Readiness, and Technical Readiness. Each section of the Readiness Guide is designed to provide I/T/U facilities with direction on evaluating and improving their facility's preparedness as they plan for modernization. The Readiness Guide also underscores that PATH EHR cannot be implemented successfully without a sustained effort from each facility. Ultimately, the value of PATH EHR lies in each end user's ability to effectively use the system to improve patient health outcomes across Indian Country.

## PURPOSE

This guide provides details on critical issues and responsibilities that organizations need to consider as they pursue a decision to join PATH EHR. Migrating from a locally managed EHR (e.g. RPMS) to an EHR that is shared by other organizations and managed as a federal data system creates significant benefits for all participants, but requires all participants follow certain practices and procedures. This document provides a high-level overview of many key issues.

This guide is not a checklist for selection into an implementation cohort, nor is it a mechanism to accelerate implementation timing. Completion of the activities described does not guarantee placement in a specific cohort. Rather, the guide is intended to help sites build internal awareness, evaluate current-state processes and infrastructure, and strengthen foundational readiness in advance of formal implementation planning.

By working through the readiness pillars described in this document, facilities can:

- Assess leadership alignment and organizational capacity
- Strengthen operational stability and workflow clarity
- Evaluate technical infrastructure and security posture
- Identify dependencies such as contracts, devices, staffing, and revenue cycle operations
- Develop a shared understanding of the scope and impact of PATH EHR
- Understand the need for a local governance structure

Implementation sequencing and cohort planning are determined through a structured, collaborative process led by the IHS Division of Health Information Technology Modernization and Operations (DHITMO) in coordination with I/T/U partners. When a site is scheduled for implementation, the team will engage directly to provide detailed guidance, timelines, and hands-on support.

Ultimately, this guide aims to enhance informed decision-making and maintain organizational readiness, ensuring that when the time comes to implement PATH EHR, each facility is positioned for a smooth transition and long-term success.

# I. ORGANIZATIONAL READINESS

## Facility and Staffing Culture

**Align facility leadership, address critical staffing needs, and plan for staff awareness.**

### Why this is important:

Understanding a facility's staffing and processes helps prepare for PATH EHR and supports the overall organizational stability needed to successfully implement the system. Every site is unique, but it is vital that a site's leadership and staffing are ready for the technical and organizational culture changes that come with PATH EHR, including the decision-making process.

Building awareness and desire to undergo this transformation is the focus for a site that is preparing to implement PATH EHR. Site executives will need to establish expectations for how facility leaders and staff will experience the implementation and deployment of PATH EHR before selection as a cohort participant. It is critical for each organization to understand the time and resource capacity for leaders and staff to support this large-scale change from current operating norms to the future state in PATH EHR.

### How to complete:

Action	Description
Align facility leadership	At this early stage, ensure executive leadership is aligned. <ul style="list-style-type: none"><li>• Establish a recurring meeting cadence (if one does not yet exist).</li><li>• Identify and plan to fill existing executive leadership vacancies.</li><li>• Complete these actions as a team.</li></ul>
Assess current-state opportunities for improvement	It is helpful for the DHITMO program team to know existing workarounds, areas of burden for end users, and known system fail points, and sites are encouraged to document these items so they can be accurately evaluated and addressed. Examples include: <ul style="list-style-type: none"><li>• <b>Clinical</b> – documentation burden, incomplete patient records, reduced system trust, etc.</li><li>• <b>Operational</b> – inefficient scheduling, incomplete revenue capture, limited reporting capabilities, etc.</li><li>• <b>IT</b> – limited scalability, complex customizations that are difficult to upgrade, limited integration capability</li></ul>
Validate the benefits of PATH EHR for your site and contextualize benefits to staff	In preparation for implementation, the DHITMO program team will provide a set of typical improvements expected with PATH EHR. Sites should be prepared to review these materials and highlight the benefits that are most relevant and resonant for their staff and patient population.

	<p>For example, benefits of a transition can focus on the:</p> <ul style="list-style-type: none"> <li>• <b>Clinical Case:</b> more workflow efficiency, increased quality of care, increased interoperability with other sites</li> <li>• <b>Operational Case:</b> increased revenue capture, operational efficiency</li> <li>• <b>IT Case:</b> increased security, systems integration, sustainability</li> </ul>
Identify and fill key staff vacancies	<p>Understand where key departmental position vacancies exist (<i>e.g., supervisors, IT staff, pharmacy staff, etc.</i>) and strategize how to fill these roles. Staff vacancies in key roles can exacerbate disruptions during implementation and deployment.</p>
Key Roles	<p>Site leadership will need to identify staff to serve in several key roles. These resources will be the primary site contacts for implementation efforts, which may be in addition to their normal daily role and responsibilities.</p> <p>The key roles outlined below highlight the functions the team aims to support. This is intended to help the deployment team understand who to involve in upcoming discussions. Roles marked with an asterisk (*) indicate areas that may benefit from being filled earlier than the others.</p> <ul style="list-style-type: none"> <li>• <b>*Implementation Site Lead</b> - Serves as the primary project contact and lead for the implementation efforts at the site.</li> <li>• <b>*Hardware Deployment Lead</b> - Plans and executes the physical deployment of hardware infrastructure required to support.</li> <li>• <b>*Subject Matter Experts</b> - Participates in data collection, build, and testing efforts as well as join the solution calls and Site Design Workshops.</li> <li>• <b>*Patient Care Location (PCL) Lead</b> - Owns the patient care location (PCL) structure of the facility.</li> <li>• <b>*Information Technology Lead</b> - Serves as the primary point of contact for all cybersecurity and technical aspects of initiatives, including events and user-reported issues related to assigned applications, networks, or systems.</li> <li>• <b>*User Role Assignment Coordinator</b> - Gathers and updates end user information and supports the user role assignment process.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Communications Lead</b> - Serves as the primary contact for distribution of communications.</li> <li>• <b>Site Training Coordinator</b> - Facilitates several key activities before and during training rollout, including site logistics, resources, and materials.</li> <li>• <b>Change Advocates</b> - Supports PATH EHR adoption as individual contributors, models ideal behaviors, helps colleagues, and promotes engagement.</li> <li>• <b>Bio-Medical Device Lead</b> - Oversees the integration, readiness, and deployment of biomedical equipment within the defined scope.</li> <li>• <b>Cutover Lead</b> - Ensures the system cutover (clinical, revenue cycle, and technical) readiness efforts in the months leading up to go-live are complete.</li> <li>• <b>Super Users</b> - A knowledge and workflow expert who supports peers undergoing PATH EHR training and implementation. They blend the people, processes, and technology to bring continuity to the end users' experience.</li> <li>• <b>Acquisitions Lead</b> – Responsible for overseeing contracts, data use agreements, software licenses, and other procurement activities at the site.</li> </ul> <p>Site staff may perform additional key functions that are integral to the implementation and deployment of PATH EHR, including but not limited to:</p> <ul style="list-style-type: none"> <li>• <b>Procurement Specialist(s)</b> – ensure timely, successful procurement for requisite system devices and interfaces owned by the site.</li> <li>• <b>Project Manager(s)</b> – serve as the primary liaison between the PATH EHR implementation team and site staff supporting the project.</li> <li>• <b>System Design Support</b> – clinical, operations, and IT staff that provide critical feedback and input for the local configuration of PATH EHR.</li> </ul>
<p>Facility leadership engagement and communication to staff</p>	<p>The executive leadership team should be prepared to create awareness among staff by providing regular PATH EHR updates during established staff meetings. Tribal and urban Indian organization executive leadership is encouraged to attend the Modernization Tribal Consultation and Urban</p>

	Confer sessions, while IHS executive is encouraged to attend the IHS Modernization Townhalls to stay informed.
--	--

## Governance

### Follow IHS governance standards while maintaining local governance structures.

#### System Governance

PATH EHR is a federal system governed by IHS policies, committees, and operational processes designed to ensure safe, secure, and effective operation of the shared electronic health record environment.

Participating organizations serve an important role in this governance process through collaboration, compliance with established policies, and participation in coordinated operational activities. Participating organizations may submit change requests or enhancement requests through established governance channels. IHS retains final authority to determine whether requested changes are approved and when they will be implemented.

#### Continuing Local Responsibilities

Participation in PATH EHR does not eliminate many responsibilities organizations have currently. Rather, participating organizations will continue to manage several core operational functions locally. For example, organizations will continue to respond to patient requests for Release of Information (ROI) in accordance with applicable laws and policies. However, internal policies and procedures related to protected health information (PHI) and personally identifiable information (PII) must be aligned with IHS policies and procedures governing the PATH EHR system. This includes the requirements described in Part 2, Chapter 7 of the Indian Health Manual. Organizations will also remain as the first line of support for providers, staff, and patients using PATH EHR services, including the patient portal. Participating organizations will provide the first level of user support, such as answering questions and helping users navigate the system. Some support functions will be handled directly by IHS. Organizations will establish internal processes to coordinate escalation of issues to the higher levels of support provided by IHS.

#### Termination

Participating Organizations may elect to “leave” PATH EHR, or transfer ownership of services currently being managed in PATH EHR. It may be possible to provide departing organizations with copies of some of the data in PATH EHR. But under no circumstances will data be removed or deleted from PATH EHR. There may be outstanding financial obligations when an organization leaves PATH EHR. There may be additional costs to provide an organization with a copy of PATH EHR data.

#### How to complete:

Enterprise governance defines standards; however, enterprise governance alone cannot address the day-to-day operational realities of a participating organization. Local governance ensures those standards work in real operations and supports consistent adoption. It should include local day-to-day functional and staffing requirements that translate enterprise standards into local operations, resolve issues, and support organizational culture. It evaluates and aligns organizational strategic requirements and priorities, costs, policy, performance, risks and compliance, responsiveness, community engagement, improves adoption,

leadership accountability, and supports patient safety.

Action	Description
Review existing local governance policy/documentation	<p>Review existing local governance documentation for management of the site’s existing EHR solution. If governance documentation does not exist, establish a team to document the local governance structure.</p> <p>If a local governance structure does not exist, one will be necessary to support and manage PATH EHR implementation and deployment.</p> <p>Local governance should include a PATH EHR decision-making body to review concerns, issues, and change requests, some of which may need to be escalated for enterprise consideration.</p>

## II. OPERATIONAL READINESS

### PATH EHR User Access

**Identify all users and their associated roles. These individuals will need a new account within PATH EHR.**

#### Why this is important:

To prepare for PATH EHR onboarding, organizations must identify all users who require access and document their associated roles. This includes reviewing current EHR users, determining whether they will need PATH EHR access, and confirming whether they already possess a valid Personal Identity Verification (PIV) card. Early identification is essential, as all PATH EHR users must meet federal access requirements—including two-factor authentication and PIV card issuance, which can take time to complete. Aligning each user’s current responsibilities with their functional role in PATH EHR ensures appropriate access levels when accounts are created.

IHS is the sole authority responsible for provisioning and managing PATH EHR user accounts, including creation, modification, suspension, and termination. Organizations must ensure that their workforce—and any third-party contractors requiring access—comply with all IHS security, privacy, and access policies. User documentation and onboarding steps must be completed promptly, as accounts inactive for 30 days may be automatically disabled.

All users must meet federal access and identity requirements, including:

- ✓ A valid need-to-know
- ✓ Completion of a federal background investigation
- ✓ Required identity verification credentials, including a PIV card
- ✓ Completion of all role-specific training
- ✓ Physical access to the system from within the United States

IHS employees and contractors generally must be U.S. citizens or meet qualified federal criteria to obtain the necessary credentials, including the PIV card. Access for contractors or third-party service providers is subject to the same standards, and organizations may be asked to share information about these arrangements.

Monitoring and audits of PATH EHR user access may occur at any time. IHS, or an authorized third party, may suspend or terminate access based on audit findings. Organizations must notify IHS of any required user access changes—including terminations, role changes, or adjustments to access levels—to allow timely updates. In emergency situations, authorized users may utilize “break-the-glass” access to view patient records necessary for immediate care. All such access is logged and audited by IHS.

Before receiving system access, all users must complete required PATH EHR training, including modules related to system use and privacy and security of PHI and PII. IHS maintains a Learning Management System to track training compliance. Some training systems may require users to have their PIV card prior to enrollment.

**How to complete:**

Action	Description
Identify personnel requiring access to PATH EHR	Identify current users and roles of existing EHR and determine if they will need access to PATH EHR. Keep a running list of names and roles. Determine if existing users have a PIV card.

## Revenue Cycle Operations

**Revenue Cycle and Purchased/Referred Care (PRC) operations must be current and remain up to date through go live.**

Revenue Cycle and Purchased/Referred Care (PRC) operations must be current based on the guidelines below:

- 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 that are 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:**

Revenue cycle operations that remain current reflect a more complete picture of an organization’s financial health, which may impact the success of PATH EHR implementation. During the implementation of the new EHR, expect a temporary reduction in patient services, which may impact the amount of revenue generated

during the transition.

Any coding, billing, and claims created in a legacy EHR must be completed in the legacy EHR. The deeper the backlogs are, the harder it is to complete, requiring the site to work in a hybrid system for a longer period. This hybrid operation increases billing backlogs in two systems, compromising the billing staff proficiency in the new patient accounting system, increasing error risk, and may materially impact cash flow and patient satisfaction. Proactive revenue cycle stabilization prior to cutover is essential to protect mutual integrity during transition.

#### How to complete:

Action	Description
EHR Facilities: Coordinate with RPMS support	Reach out to your EHR Resource and Patient Management System (RPMS) support team for assistance.
Non-EHR Facilities: Collaborate with Revenue Cycle manager(s)	Work with your Revenue Cycle manager(s) to determine how revenue cycle operations should be managed for your EHR.

## Data Migration Preparedness

### Ensure your legacy system is current on its certified software maintenance.

To prepare for migrating data from the legacy system to PATH EHR, sites need to ensure their legacy system is current on their certified software maintenance packages or patches. For RPMS systems, this includes ensuring your system has the most recent release of the RPMS/Ensemble Cache Classes Database File (BMW) CACHE.DAT installed on the system.

To prepare the legacy data for migration, perform the following:

- Resolve common data issues
  - Logical Observation Identifiers Names and Codes (LOINC), RxNorm nomenclature, National Drug Codes (NDCs), Current Procedural Terminology (CPT) codes, etc.
- Maintain the Integrated Problem List (IPL)
  - Map problems to Systematized Nomenclature of Medicine – Clinical Terms (SNOMED)
  - Maintain the IPL for accuracy through migration
- Identify data that requires special handling, such as but not limited to:
  - Substance abuse treatment records
  - Behavior health provider notes
  - Employee health records
  - Confidentiality/Sensitive data
- Identify processes for handling special data
  - Provide list of special handling data
  - Assist with creating the methods necessary to identify the elements during migration

#### Why is it important:

Ensuring that a health system is fully updated prior to migrating data to a new system is essential to

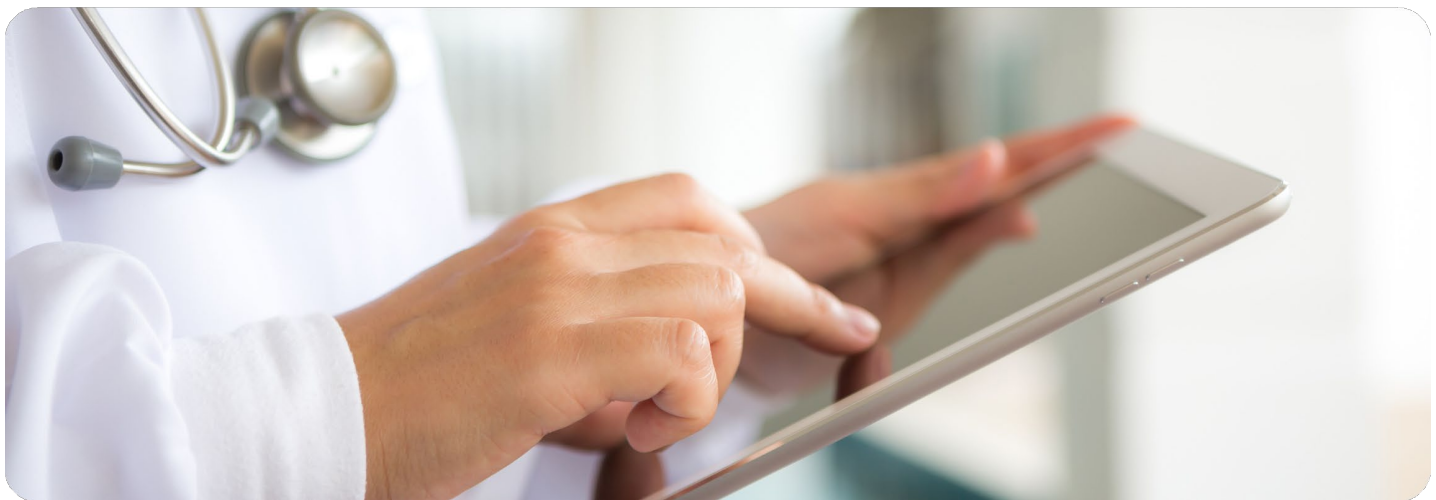
safeguarding patient safety and maintaining regulatory compliance. System updates help preserve data integrity, prevent data loss, and support operational continuity and compatibility with PATH HER. They also reduce clinical risk, minimize downtime and post-migration remediation efforts, enable accurate reporting and analytics, and maintain appropriate chain of custody and audit trails. In healthcare, data accuracy directly impacts care delivery, quality outcomes, and reporting obligations, making system readiness a critical prerequisite to any migration initiative.

## Clinical Data Clean Up

**Conduct a comprehensive review and update of all existing medication, allergy, and problem list data within the current system to ensure accuracy, completeness, and clinical reliability.**

How to complete:

Action	Description
Reconcile medications during patient interactions	Use existing workflows to review and confirm current medications at each patient visit or chart review.
Verify allergy details	Ensure allergy information is up to date by checking and confirming details during patient visits or chart reviews.
Confirm active problem lists	Review and validate the list of ongoing medical problems during patient interactions to ensure accuracy.
Engage clinical staff for validation	Involve clinical staff to validate the accuracy of entries and ensure outdated or duplicated information is removed from records.



## Clinical and Administrative Workflows Review

**Review clinical and administrative workflows.**

Reviewing both clinical and administrative workflows before EHR implementation ensures your site: improves efficiency while avoiding new issues, enhances patient safety, reduces staff resistance, maximizes return on investment and supports high-quality patient care.

### Why this is important:

Reviewing current workflows before EHR implementation is critical because it ensures the system supports how clinicians and staff actually deliver care. Without evaluating existing processes, organizations risk digitizing inefficient workflows, increasing documentation burden, and creating safety risks. Workflow analysis helps identify bottlenecks, eliminate duplication, improve patient safety, and configure the EHR to match clinical needs. It also promotes staff engagement and smoother adoption. Ultimately, reviewing workflows ensures that the EHR enhances efficiency and quality of care rather than disrupting operations.

### How to complete:

Action	Description
Identify current workflow inefficiencies and bottlenecks	Workflow review will help to uncover: <ul style="list-style-type: none"><li>• Duplicate documentation</li><li>• Manual steps that can be automated</li><li>• Delays in communication</li><li>• Unnecessary approvals or handoffs</li></ul>
Involve staff in workflow analysis	Staff are more likely to embrace change when they feel heard. This also supports buy-in, reduces resistance, improves adoption, and identifies training needs.

## III. TECHNICAL READINESS

### Identify Service Lines

**Identify the existing Service Lines supported by the site and the systems the site uses to provide those services.**

### Why this is important:

Each Service Line provided by a site will be impacted by the implementation of PATH EHR. It is critical to identify all existing service lines, as well as planned expansions to these service lines prior to implementation to ensure all services can be comprehensively planned for transition to PATH EHR.

Examples of Service Lines include, but are not limited to: Primary Care, Internal Medicine, Women's Health, Pediatrics, Laboratory, Pharmacy, Radiology, Ophthalmology, and Infusion Services. Also consider any other specialty clinics the facility supports throughout the year, such as vaccination events or community health screenings.

### How to complete:

Action	Description
Identify Service Lines required to be supported by PATH EHR	Identify current Service Lines provided at the site and any planned expansions of service. Identify the current

	individual primarily responsible for the oversight of each Service Line.
Identify systems supporting each Service Line	List each system currently supporting each Service Line. Include the name of the product and whether or not it is currently connected to RPMS or other system that connects to RPMS.

## Devices and Interfaces

### Identify ports, protocols, and interfaces on all devices, peripherals, and biomedical equipment at your facility.

#### Why this is important:

PATH EHR is a shared system composed of multiple integrated technologies, including software applications, infrastructure components, medical devices, and system interfaces. Some components of PATH EHR are required for all participating organizations, while others are optional, depending on the services provided by the organization. Compatibility between PATH EHR and an organization’s existing systems or devices will be determined during the Discovery phase, where technical integration needs are evaluated. IHS serves as the final authority regarding which devices and technologies may connect to the PATH EHR environment.

This information is vital to the integration and interoperability of the new EHR. It will assist in defining what PATH compatible interfaces and devices can be utilized for integration and interoperability at a local site. Having compatible devices helps define the level of effort for the PATH implementation as well as define devices that need replacement. This information supports compliance with cybersecurity and regulatory standards; facilitates accurate planning for network segmentation, bandwidth requirements, and integration dependencies, and reduces the risk of service interruptions during deployment. Comprehensive documentation of these communication requirements also streamlines vendor coordination and enhances long-term maintainability and troubleshooting.

Only IHS-approved and/or licensed software and hardware may be used with PATH EHR. This ensures that all systems connected to PATH EHR meet federal security and interoperability standards. Organizations may need to replace or upgrade certain equipment if it does not meet PATH EHR requirements. In some cases, existing systems or devices may not be compatible with the shared EHR environment.

Participating organizations are responsible for purchasing and maintaining certain end-user equipment, such as workstations, tablets, and local devices used by staff. Organizations are also responsible for purchasing and maintaining sufficient and reliable network connectivity to PATH EHR. IHS is responsible for managing and maintaining the core infrastructure and centralized components of the PATH EHR system.

## How to complete:

Action	Description
Compile a complete asset inventory	List all third-party interfaces, integrated devices, peripherals, and medical equipment (including network-attached and non-network-attached items, such as biomedical devices, pharmacy cabinets, robotics, and lab instruments).
Inventory third-party interfaces	The interface inventory should contain details such as the system and vendor name, interface type (e.g. HL7, FHIR, DICOM), ports, protocols, and standards used, and direction of data flow. An inventory template is included for your convenience in the appendix.
Inventory devices, peripherals, and medical equipment	The list should include: <ul style="list-style-type: none"><li>• device name</li><li>• device type</li><li>• model number</li><li>• software/firmware version</li><li>• connection type (if connected to an existing system)</li><li>• associated maintenance contract</li><li>• device location in the facility</li></ul>
Review compatibility with PATH EHR	If planning upgrades or new device/interface acquisitions, review the appendix for the list of devices and interfaces compatible with PATH EHR to ensure alignment.

## Contracts, Agreements, and Licenses

**Identify all contracts and their associated refresh cycles. Where possible, ensure the agreements are up to date.**

### Why this is important:

Contracts and data agreements that need to be reviewed for accuracy and verified to be current 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, third-party interface system support, and medical device maintenance contracts. If your site is involved in clinical trials or research studies with drug companies, review the agreements for those activities including but not limited to clinical trial procedures and data collection timelines.

### Contracts

If implementing the new EHR requires changes to existing health IT or biomedical equipment contracts, begin by working with your contracting officer(s) to notify current vendors that your facility is exploring preparation options for migrating to the IHS PATH EHR (Oracle Health Millennium). The DHITMO program team can provide recommendations throughout the implementation process on the contract modifications or new

acquisitions that your facility may need to submit to your contracting office. However, each site's acquisition needs will vary based on the services provided. In addition, the IHS PATH EHR is an Enterprise EHR, and certain interfaces that a facility manages today may transition to the Enterprise's responsibility for maintenance and associated contracting.

Knowing device and interface contract refresh cycles will help preemptively identify potential implementation delays or disruptions due to new implementations or unexpected upgrade requirements. This research should identify contracts/agreements that will no longer be needed in the new environment, those that should continue with some modification, and those that should continue as is. Possessing a comprehensive list of contracts and associated assets or services assists in that process and can aid in identifying where new vendors or services may not need to be purchased.

### Data Agreements

Information stored in PATH EHR may be subject to multiple legal requirements, including federal, state, tribal, and contractual privacy and security obligations. When multiple standards apply, all applicable requirements must be followed. If requirements differ, all participants will endeavor to apply the most protective standard to govern the use, disclosure, and safeguarding of the information. Data agreements, such as interconnection security agreements (ISA) and data exchange agreements (DEA) 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.

### Interparticipant Agreements

Participating Organizations may enter into written agreements granting other Participating Organizations specific rights to access or use Financial Information or proprietary information. All such agreements must comply with applicable federal, state, tribal, and contractual requirements ("Legal Obligations") and must be consistent with PATH EHR governance standards, including data stewardship, minimum necessary use, and role-based access control principles. Portions of such contracts may need to be shared with IHS to provide the appropriate level of access to PATH EHR.

### Third-Party Agreements

Participating Organizations may enter into written agreements granting Third-Parties specific rights to access PATH EHR to provide services on behalf of the participating organization. All such agreements must comply with applicable federal, state, tribal, and contractual requirements ("Legal Obligations") and must be consistent with IHS Data Use Agreement requirements, PATH EHR governance standards, including data stewardship, minimum necessary use, and role-based access control principles. Portions of such contracts may need to be shared with IHS for IHS to provide the appropriate level of access to PATH EHR.

### How to complete:

The following recommended actions will facilitate early information sharing and current-state assessments that are conducted during the preliminary phases of implementation. An optional template for collecting this information is provided in the Appendix.

Action	Description
Identify contracted services and existing agreements	List all currently contracted services that support the medical services provided at the facility, such as: Radiology (PACS, teleradiology, imaging devices), Laboratory (reference labs, lab analyzers), Pharmacy (medication dispensing), services, medical devices (biomedical, lab, pharmacy), printer and multi-function device lease/maintenance agreements, endpoint (workstation) device lease/refresh/maintenance agreements, operating systems (Registries, HIEs, TECs, etc.)
Compile contract documentation (Tribal or Urban Organizations may use different terms for items on this list; please adapt the data collection tool as needed)	<p>For each identified contracted service, provide documentation on: contract renewal periods, contract/agreement management points of contact, specialized reporting requirements, if contract is shared with other sites, etc.</p> <p>The following items should be included:</p> <ul style="list-style-type: none"> <li>• Contract ID</li> <li>• Period of Performance and Terms</li> <li>• Number of Option Years</li> <li>• Total Contract Value (for all years)</li> <li>• Type of Contract</li> <li>• Brief Scope description</li> <li>• Contracting Office</li> <li>• Contracting Officer</li> <li>• Contracting Officer Representative</li> <li>• Vendor</li> </ul>

## Planned Upgrades, Implementations, and Renovations

### Identify any significant software or hardware implementations and major planned facility renovations.

#### Why this is important:

Significant software or hardware updates may change current system compatibility, performance or result in a change in requirements. Identifying major upgrades or implementations planned for the foreseeable future will help uncover potential configuration needs or requirements that can be addressed early, enabling better schedule alignment, ensuring compatibility, and minimizing potential conflicts.

Facility renovations may influence PATH EHR implementation by altering physical layouts, impacting network connectivity, and limiting access to installation sites. Knowing about facility renovations will enable the DHITMO program team to provide recommendations that align with best practices to ensure facility upgrade projects will be inclusive of optimization for PATH EHR success (e.g. including power upgrades).

### How to complete:

Action	Description
Identify planned facility renovation projects	List upcoming facility renovation projects for the foreseeable future. Specify the project, the need being addressed by the renovation, impacted service line(s) or location(s), and planned start/completion dates.
Identify planned, significant software, biomedical devices, or infrastructure hardware upgrades/implementations	List significant software/hardware upgrade or implementation projects planned within the next 18-24 months. Include what software, biomedical devices, or hardware is scheduled for upgrade, the need being addressed by the upgrade, which service line(s) or location(s) is impacted, and the planned start/completion dates.
If considering device/interface upgrades or acquisitions	Review the list of devices and interfaces compatible with PATH EHR (as found in the document appendix). Ensure that any planned upgrades or new acquisitions align with this compatibility list.

## Network Infrastructure of Legacy Electronic Health Records

### Update your legacy EHR system to the latest version.

#### Why this is important:

An updated infrastructure helps keep your data secure and systems operating as efficiently 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 seamless transition. Focusing on the network infrastructure is essential because it forms the underlying foundation that supports all clinical, operational, and administrative systems within a facility. A thorough assessment of the network ensures that bandwidth, segmentation, wireless coverage, cabling, switching, routing, and security controls are capable of supporting current and planned workloads, including high-dependency systems such as PATH EHR, biomedical devices, and imaging systems. Evaluating the network in advance helps prevent performance bottlenecks, ensures compliance with security and regulatory requirements, reduces the risk of service disruptions during deployment, and provides the necessary visibility to plan upgrades or mitigations proactively.

### How to complete:

Action	Description
For RPMS users: Access certified IHS applications	View the latest IHS-certified applications specific to RPMS users at the designated IHS resource.
For commercial EHR users: Check for the ONC Certified Health IT Product List	Identify the most recent certified version of your commercial EHR software using the ONC Certified Health IT Product List website.

## 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 PATH EHR may be accessed or utilized.

Reviewing the activity and status of your facility's network allows you to identify and promptly 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 robust, efficient, and secure network infrastructure in your facility.

### How to complete:

Action	Description
Conduct a comprehensive wireless site survey	Assess wireless networking performance throughout the facility to identify weak signal areas or interference.
Evaluate wired network performance by using network monitoring tools	Evaluate wired network performance by checking routers, switches, and access points for bottlenecks or failures.
Test wireless connectivity with end-user devices	Perform thorough testing at various facility locations using devices meant for EHR-related functions. Note signal strength, latency, and packet loss. Consult the appendix for a list of PATH EHR-compatible devices.
Verify device configuration and all firmware/drivers are updated	Ensure all network devices have proper configurations and up-to-date firmware/drivers. Confirm sufficient bandwidth for anticipated needs.
Conduct periodic security audits	Regularly audit network security to prevent unauthorized access and identify vulnerabilities. Establish redundancy and failover (e.g., dual internet providers) for resilience.
Reassess and optimize network configuration	Continuously review and adjust network setup based on facility requirements.
Maintain and update network diagrams	Network Operations Security Center (NOSC) should have current diagrams for federal facilities; local staff should maintain diagrams for tribal/urban sites. Create new diagrams if none exist, with help from NOSC or network staff.

Check network status with NOSC (IHS facilities)	From within the IHS network, use the NOSC portal to monitor your network's health and status.
Gather local network information (tribal/urban facilities)	If NOSC information isn't available, have onsite staff produce reports or gather data to assess local network activity and status.



## Network Security Audits and Reviews

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

### Why this is important:

Participating organizations must implement and maintain administrative, technical, and physical safeguards to protect PATH EHR data. Network Security audits and reviews are essential for the IHS infrastructure to be secure, compliant, and resilient against cyberattacks. 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 six concurrent and continuous functions: Govern, 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 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.

Organizations are required to conduct a Security Risk Assessment (SRA) at least annually and address any identified risks or vulnerabilities. IHS may request copies of these assessments to ensure alignment with federal security standards.

Organizations must also comply with IHS security requirements for:

- Networks
- Mobile devices
- End-user devices
- Biomedical devices connected to the system

Organizations may be asked to provide information regarding major security incidents occurring within recent years as part of the onboarding or readiness process.

### Monitoring and Compliance

IHS will operate tools that support monitoring, alerting, and compliance investigations within PATH EHR. In some cases, organizations may receive access to monitoring tools that help track compliance alerts and system events. When organizations are granted access to these tools, they are expected to use them to monitor activity and assist with investigations when necessary. Organizations and IHS will cooperate in responding to compliance or security concerns.

### Security Incident Reporting

Participating organizations must promptly notify IHS if they become aware of:

- Security incidents
- Unauthorized system access
- Suspected or confirmed breaches
- Theft or compromise of computer systems

Organizations and IHS will work together to investigate and respond to such events.

### Breach Investigations

If a breach is suspected, organizations must notify IHS as quickly as possible. IHS will lead the breach investigation and coordinate with affected organizations. Organizations must designate highly available points of contact to assist in the investigation process until the incident is resolved. IHS may suspend or terminate user, organizational, or system access if necessary to protect system integrity or patient information.

How to complete:

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

## Network Policies and Guidelines for Electronic Protected Health Information (ePHI)

### Conduct a security hardening assessment using relevant NIST standards and control baselines.

#### 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.

#### Access to Patient Information

Participating organizations may access, use, and disclose PHI within PATH EHR for treatment purposes, consistent with HIPAA, the Privacy Act, and other applicable laws. Organizations may view information entered by other participating organizations only when necessary to support the care of patients they treat. Such access is limited to minimum necessary use and permitted healthcare operations. Employee health records must be maintained separately from patient health records and may not be stored in PATH EHR.

#### Reporting and Analytics

Individuals granted access to certain reporting and analytics features may have access to data from multiple organizations. A high level of trust and training is required for those granted this access. The development of new reports and analytics will require a change request to IHS following governance processes.

#### Use of Data for Research

Participating organizations may not use data generated by another organization within PATH EHR for research purposes without explicit written authorization from the originating organization. Additional federal review requirements may apply. The procedure outlined in the Indian Health Manual applies.

#### Permissible Use of PATH EHR by IHS

IHS may use and disclose PATH EHR data in compliance with Federal law to support PATH EHR, perform administrative functions and data aggregation services on behalf of Participating Organizations, and other services required by law and regulation, provided such use and disclosure comply with applicable privacy, security, and confidentiality laws.

#### Accreditation, Survey, and Inspection Response

IHS will establish a standardized process for providing access to resources for rapid-response support when external agencies conduct audits, reviews, inspections, or similar oversight activities involving an organization, and when assistance from IHS personnel or contractors is required. The Participating Organization will provide IHS with as much advance notice as possible of any anticipated inspection or audit.

### Insurance Considerations

Participation in PATH EHR may affect an organization's cybersecurity insurance policies or coverage requirements. Organizations are encouraged to consult their insurance providers.

### Legal Requests for Data

Recognizing that PATH EHR is a federal data system, if an organization receives a legal request for patient information (such as a subpoena or court order), the organization will work with IHS to review the data request and the appropriate policies and procedures to follow. If the request includes information created by another organization, IHS will coordinate the response.

### Patient Requests for Amendments

Organizations may amend only the patient records that were created at their facilities. When corrections are made, organizations will notify IHS so that changes are appropriately reflected within PATH EHR. Organizations should follow the Procedure for Requests for Correction/Amendment of PHI in the Indian Health Manual.

### Patient Requests for Accounting of Disclosures

When patients request an accounting of disclosures, organizations will provide records for disclosures made by their own organization. IHS may assist organizations in fulfilling these requests. Accounting of disclosures must be made in accordance with the policies and procedures outlined in the Indian Health Manual Part 2, Chapter 7.

### Patient Requests for Restrictions

Participating Organizations shall make their own independent determination, in response to patient requests, whether to grant or deny requests to restrict access to PHI. Organizations may only restrict access to users at their organization and not users at another organization.

### Patient Record Merges

Because PATH EHR is a shared system, merging duplicate patient records carries significant risk. IHS has final authority to determine whether a patient record merge will occur and will manage the process when approved.

### Privacy Notices

Organizations may need to update their Notice of Privacy Practices (NPP) to reflect PATH EHR participation and applicable federal requirements. IHS may provide required language or standardized notices to ensure compliance with federal laws and the capabilities of the PATH EHR system.

## How to complete:

Action	Description
Review the NIST Cybersecurity Framework	Examine the referenced NIST Cybersecurity Framework as it applies to healthcare to ensure your organization's practices align with recommended standards.
Address Discrepancies	Identify and take corrective action for any gaps or misalignments between your current practices and the framework's requirements.
Document Findings	Record all findings, including identified discrepancies and the steps taken to resolve them, for ongoing compliance tracking and audit readiness.
Update downtime procedure	A downtime procedure defines what to do and how to document patient care when the system or the infrastructure does not work during an outage.

## Stay Connected

**Regularly review the IHS Health IT Modernization Program website, blog, and social media pages, attend events, and join the Modernization listserv.**

### 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. 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:

#### Focus Groups

- To participate an upcoming focus group or receive general participation information about volunteer opportunities, email [modernization@ihs.gov](mailto:modernization@ihs.gov).

#### Tribal Consultation/Urban Confer (TC/UC)

- Register to attend an upcoming event and view presentations from past events at [IHS.gov/HIT/Events](https://www.ihs.gov/HIT/Events).

#### Online Resources

- Navigate to [IHS.gov/HIT/Resource-Hub](https://www.ihs.gov/HIT/Resource-Hub) to access documents, presentations, modernization program blog posts, modernization Tribal/Urban Leader letters, modernization video series, and social media.

## **GLOSSARY**

### **BMW**

RPMS/Ensemble Cache Classes Database File (BMW) CACHE.DAT

### **COTS**

Commercial Off-the-Shelf

### **CPT**

Current Procedural Terminology

### **DEA**

Data Exchange Agreement

### **Deployment**

The final phase of transitioning a developed product, system, or service into live production and operational use.

### **DHITMO**

Division of Health Information Technology Modernization and Operations

### **DICOM**

Digital Imaging and Communications in Medicine

### **EHR**

Electronic Health Record

### **ePHI**

Electronic Protected Health Information

### **FHIR**

Fast Healthcare Interoperability Resources

### **HIE**

Health Information Exchange

### **HIPAA**

Health Insurance Portability and Accountability Act

### **IHS**

Indian Health Service

### **Implementation**

The project phase involving mobilizing resources, managing teams, and executing tasks defined in the project plan to achieve specific objectives.

### **IPL**

Integrated Problem List

**I/T/U**

Indian Health Service, tribal, and urban Indian organization partners

**ISA**

Interconnection Security Agreement

**LAN**

Local Area Network

**LOINC**

Logical Observation Identifiers Names and Codes

**MOA**

Memorandum of Agreement

**MOU**

Memorandum of Understanding

**MPA**

Master Participation Agreement

**NDC**

National Drug Code

**NIST**

National Institute of Standards and Technology

**NOSC**

Network Operations Security Center

**NPP**

Notice of Privacy Practices

**PACS**

Picture Archiving and Communication System

**PCL**

Patient Care Location

**PHI**

Protected Health Information

**PII**

Personally Identifiable Information

**PIV**

Personal Identity Verification

**PRC**

Purchased/Referred Care

**ROI**

Release of Information

**RPMS**

Resource and Patient Management System

**SAS**

Security Agreement Summary

**SNOMED**

Systematized Nomenclature of Medicine – Clinical Terms

**TEC**

Tribal Epidemiology Center

**UFMS**

Unified Financial Management System

**WAN**

Wide Area Network

**APPENDIX**

To request any of these documents, please email [IHSDHITMOComms@ihs.gov](mailto:IHSDHITMOComms@ihs.gov).

Local Governance Guide

PATH EHR Compatible Devices and Interfaces

Third-Party Interface Inventory Template

Contract Inventory Template

Data Management Strategy

