WHITE PAPER

From data exchange to operational interoperability

Why moving data isn't enough



Table of contents

01. Introduction 3

02. Connectivity has become the baseline 4

03. From technical interoperability to operational interoperability 5

04. The EHR is central, but not the entire interoperability strategy 7

05. The hardest problems often appear after go-live 8

06. The architecture is layered, not either/or 10

07. Trust is a managed data lifecycle 11

08. The operating model matters as much as the technology 12

09. Where healthcare organizations should start 13

10. Building operational interoperability across the enterprise 15

11. What leaders should measure 17

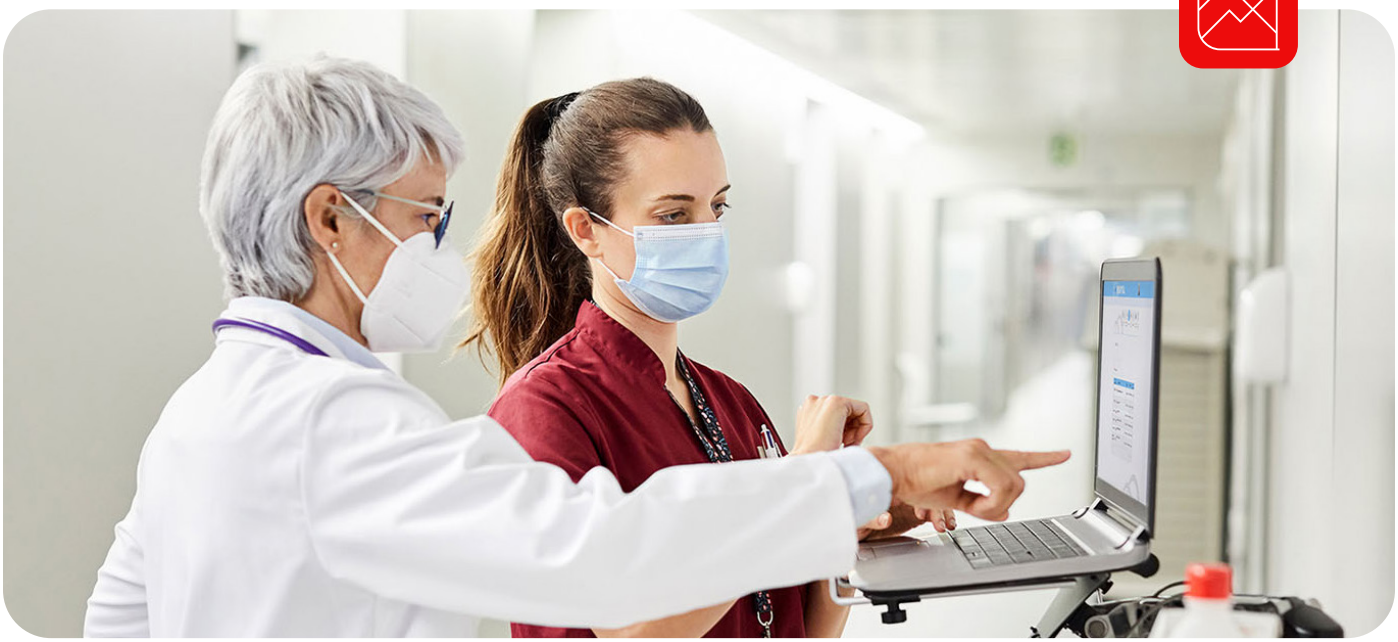
12. Conclusion: The endpoint is the beginning 18

Introduction

In 2024, the Centers for Medicare & Medicaid Services (CMS) released the Interoperability and Prior Authorization Final Rule, CMS-0057-F, requiring impacted payers to implement or expand four FHIR-based APIs. While exchanging healthcare data is not new, the expectation that the information be standards-based, consistently accessible and usable across organizations and workflows marks an important shift.

Meeting the requirement will demand significant investment. It also creates an opportunity to build a foundation that extends beyond a single mandate or API. Moving data is not the same as making it useful. An endpoint can be live while the information is incomplete, its context remains unclear, or the workflow on the other side does nothing with it.

The next step is to move from technical interoperability, the ability to exchange data, to operational interoperability, the ability to turn exchanged data into trusted decisions, repeatable workflows, and measurable outcomes. This paper explores what sits between an endpoint and an outcome, and how each investment can make the next one easier.



Connectivity has become the baseline

For decades, interoperability programs were judged by whether systems could exchange information at all. The milestone was understandable: establish the interface, make the route reliable, validate the transaction, and keep it running. That engineering work remains essential. But at this point in the industry, connectivity alone is no longer a reliable metric for whether the business or clinical objective has been met.

Recent national data illustrates the shift. The Assistant Secretary for Technology Policy and Office of the National Coordinator for Health IT (ASTP/ONC) reported that in 2024, roughly nine in ten hospitals gave patients access to their health information through an API, and about seven in ten did so through standards-based APIs. At the same time, hospitals' exchanges with third-party technology for clinical and administrative purposes still ran on a mix of standards-based APIs, proprietary APIs, and other methods.[1]

This is not evidence that interoperability is finished. It shows the industry has entered a more mature phase. The key question is shifting from "Can we connect?" to "Can the connection produce reliable, reusable operational value?"

The connectivity fallacy

A common architecture mistake is to equate successful transport with successful interoperability. The two are related, but they are not equivalent.

TECHNICAL CONNECTIVITY PROVES	OPERATIONAL INTEROPERABILITY MUST PROVE
An endpoint exists	The correct endpoint or partner can be discovered
A connection was established	The relationship can be maintained reliably
A payload moved	The required data is complete and usable
A standard was used	Meaning is consistent for the intended use
A transaction completed	The correct workflow acted on it
A requirement was addressed	The organization realized measurable value



A successful transaction tells us that data moved. It does not tell us whether anything useful happened.

1. Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP/ONC). "Hospital Use of APIs to Enable Data Sharing between EHRs and Third-Party Technology." Data Brief No. 81, February 2026. https://healthit.gov/data/data-briefs/hospital-use-of-apis-to-enable-data-sharing-between-ehrs-and-third-party-technology/

From technical interoperability to operational interoperability

Standards solve indispensable problems. They define structures, interactions, terminology bindings, security patterns, and implementation expectations that make exchange more predictable. HL7 describes FHIR as a standard for exchanging healthcare information electronically and explicitly notes that FHIR can be used on its own or in partnership with widely used standards such as HL7 Version 2 and CDA.[2]

That last point is critical. Healthcare is not moving from one monolithic interoperability era into another. Most organizations operate heterogeneous environments containing long-lived message flows, documents, batch processes, APIs, event streams, partner-specific exchanges, and FHIR-based access patterns. The architectural goal should not be to force every workload through the newest technology. Instead, it should create a coherent operating model in which each exchange pattern is used appropriately, and the resulting information can be trusted and reused.



Redefining interoperability success: Operational interoperability is the ability to connect the right parties, exchange the right information, preserve its meaning and context, route it into the right workflow, handle exceptions, and demonstrate the intended outcome.

Five capabilities sit between an endpoint and an outcome



Connection

The organization can discover, establish, secure, monitor, and maintain the exchange relationship.



Trust

The receiving party can determine whether the data is complete, accurate enough, consistent, traceable, and fit for the intended use.

2. HL7 International. "FHIR Overview," FHIR Release 5 (v5.0.0). https://hl7.org/fhir/overview.html

Context

Identity, terminology, provenance, timing, source, and purpose are preserved well enough to support interpretation.

Workflow

The information reaches the correct process, person, service, or automated decision point, with clear exception handling and accountability.

Scale

The organization can repeat the pattern across partners, systems, use cases, and transaction volumes without creating a new one-off integration burden each time.

For healthcare leaders, the practical implication is straightforward: start with a high-value workflow and define the information and decisions it requires. Then build the underlying capabilities so they can be reused across additional partners and use cases.



The EHR is central, but not the entire interoperability strategy

The EHR is central to healthcare interoperability. Modern EHR platforms provide substantial interoperability capabilities, including traditional interfaces, APIs, FHIR, external data exchange, patient and provider access, and native clinical workflows. Healthcare organizations should take full advantage of these capabilities.

The distinction is that EHR interoperability and enterprise interoperability are not necessarily the same thing. The EHR is a critical source and destination within a broader ecosystem that also includes laboratories, imaging, specialty clinical systems, medical devices, payer and HIE relationships, ERP and revenue-cycle platforms, enterprise analytics, data platforms, acquired systems, and AI and digital-health partners.

EHR INTEROPERABILITY CAN PROVIDE	ENTERPRISE INTEROPERABILITY MUST EXTEND ACROSS
Interfaces, APIs, FHIR, external exchange, and native connectivity	The full ecosystem of EHRs, labs, imaging, specialty systems, devices, payers/HIEs, ERP, revenue cycle, data platforms, and external partners
Access to EHR-held clinical data and EHR-native workflows	Multi-source data and workflows that cross organizations, business functions, and technology domains
Identity, terminology, context, and governance within the EHR's operating boundary	Enterprise identity resolution, normalization, provenance, quality controls, and governance across sources
Clinical workflow support within the EHR	Orchestration across clinical, administrative, payer, analytics, population health, and partner workflows
Vendor-specific ecosystem and lifecycle capabilities	Reusable interoperability services that operate consistently across vendors, partners, acquired systems, and new use cases

Many of the highest-value healthcare use cases are inherently cross-system. A quality program may require clinical information from the EHR, external lab results, attribution data, and payer information. A population-health workflow may combine information from multiple hospitals and external partners. As these use cases become more connected, enterprise interoperability must do more than exchange information. It must connect and route data across systems, normalize it where necessary, and govern what happens next.

The hardest problems often appear after go-live

A production endpoint can create a false sense of completion. In practice, go-live is usually when organizations begin to uncover how the data and workflow actually perform in operation.

Discovery and lifecycle management

An endpoint is useful only if the right party can identify it, establish trust, authenticate appropriately, and keep the relationship current. Certificates expire. Partner configurations change. Organizations merge. Network routes evolve. Access policies change. Endpoints are versioned, replaced, or retired.

At enterprise scale, these are not implementation details; they are lifecycle management requirements. A scalable interoperability program therefore needs inventory, ownership, monitoring, change management, and operational observability around the exchange itself.



Data can validate and still be unusable

Conformance is necessary, but it is not the same as fitness for purpose. A resource may be structurally valid while a required observation is missing. A code may be technically permitted, but its meaning may be too local for the receiving organization. A date may be present but represent a different clinical moment than the downstream workflow expects.

Trust has multiple dimensions:

- **Completeness:** Are the data elements required for the intended use present?
- **Consistency:** Are values represented in a predictable way across sources and encounters?
- **Terminology:** Can both sides interpret coded concepts consistently?
- **Identity:** Are patients, members, providers, organizations, and devices matched correctly?
- **Timeliness:** Is the information current enough for the decision being made?
- **Provenance:** Can the source, time, transformation history, and ownership of the data be understood?
- **Fitness for purpose:** Is the data sufficiently reliable for this specific clinical, administrative, analytical, or AI use case?

Workflows are where value is created or lost. Even trusted data creates no value if it stops at the integration boundary. Operational interoperability requires an explicit answer to what happens next.

- Which workflow receives the information?
- What decision or action should occur?
- Who or what is accountable for that action?
- What happens when required information is missing or contradictory?
- How are exceptions surfaced, routed, and resolved?
- How is the outcome documented and measured?

These questions apply whether the use case is care coordination, quality measurement, population health, revenue cycle automation, partner data exchange, clinical decision support, or AI. The transport mechanism changes; the operating problem does not.

The architecture is layered, not either/or

Modern interoperability should be designed as a layered enterprise capability rather than as a debate between legacy interfaces and FHIR. The most durable architecture preserves proven operational flows while adding standards-based access, stronger normalization, reusable services, governance, and workflow orchestration.

LAYER	PRIMARY ROLE	REPRESENTATIVE CAPABILITIES
Outcomes	Where value is realized	Clinical workflows, administrative automation, analytics, population health, digital ecosystem services, AI
Standards-based access	Reusable access and exchange	FHIR resources, APIs, partner access, security, authorization
Trust and context	Make data safe and usable	Validation, terminology, identity, provenance, data quality, governance
Integration and orchestration	Move and coordinate information	Routing, transformation, messaging, documents, events, workflow orchestration, monitoring
Operational systems	Systems of record and execution	EHRs, labs, imaging, payer platforms, revenue cycle, ancillary and specialty systems

This model also explains why FHIR should not be positioned as a wholesale replacement for integration engines. FHIR creates standardized information models and access patterns. Integration engines remain valuable for event-driven routing, transformations, message-based workflows, partner connectivity, monitoring, and the many exchange patterns that are not being replaced simply because APIs are more widely available.



The question for organizations is therefore not which technology wins, but which layer owns which responsibility and how to prevent responsibilities from being duplicated or falling between layers?

Trust is a managed data lifecycle

Organizations often treat data quality as a cleanup activity performed after an exchange is built. That approach does not scale.

Trust must be designed into the interoperability lifecycle:

- **Ingest:** Receive data from internal and external operational sources.
- **Transform:** Convert structure or representation where necessary without losing meaning.
- **Normalize:** Align terminology, units, identifiers, and reusable representations.
- **Expose:** Make information available through the appropriate standards-based or operational access pattern.
- **Enrich:** Add context required for interpretation, routing, or decision-making.
- **Validate:** Evaluate conformance, completeness, plausibility, and use-case requirements.
- **Orchestrate:** Route information into the workflow, decision, or downstream service that needs it.
- **Observe:** Monitor quality, latency, exceptions, usage, and outcomes over time.

Governance must be executable

Governance is often discussed as policy. Operational interoperability requires governance to become executable: named owners, defined quality thresholds, version management, data contracts, escalation paths, traceability, and clear decisions about what is acceptable for each use case. This does not mean every data element must be perfect. It means the organization should be able to state what “good enough” means for a particular decision and detect when the data falls below that threshold.

The operating model matters as much as the technology

Operational interoperability depends on more than architecture. Technical teams must establish reliable exchange, but clinical and business leaders must determine whether the information is meaningful, appropriate for the workflow, and useful to the people responsible for acting on it. Programs become fragile when any of these perspectives is missing.

The five capabilities described earlier also provide a way to assess interoperability maturity. As organizations strengthen connection, trust, context, workflow, and scale, they move from successfully exchanging data to using it consistently across decisions, workflows, and emerging use cases. The following model is intended as a practical management framework rather than an industry certification.

STAGE	PRIMARY QUESTION	EVIDENCE	COMMON FAILURE MODE
Connected	Can data move reliably?	Endpoints, interfaces, routes, security, uptime	Transport success is mistaken for business success
Trusted	Can the data be relied upon for the intended use?	Quality rules, terminology, identity, provenance, validation	Valid payloads are incomplete or ambiguous
Operational	Does the exchange drive the right workflow?	Routing, accountability, exception handling, auditability	Data arrives but requires manual rescue
Scalable	Can the capability be reused broadly?	Reusable services, lifecycle management, observability, standard patterns	Each new partner becomes a custom project
Intelligence-ready	Can data safely support analytics and AI?	Governance, traceability, context, monitoring, fit-for-purpose controls	AI projects become data remediation projects

Where healthcare organizations should start

The most effective modernization programs begin with a high-value workflow and work backward to the data, partners, architecture, and controls required to make that workflow reliable. Starting with a technology mandate can produce infrastructure without a clear operating outcome.



Define the outcome first

Choose a specific clinical, administrative, analytical, or partner workflow and define what success looks like in operational terms.



Map existing integrated assets

Determine which interfaces, documents, APIs, FHIR services, identity capabilities, terminology services, and monitoring tools already solve part of the problem.



Map the decision path

Identify who or what receives the information, which decisions occur, what exceptions are possible, and where accountability sits.



Identify the minimum trustworthy data

Define the data elements, terminology, context, identity, provenance, and timeliness the use case needs, rather than aiming for an abstract ideal of perfect data.

Separate transport from trust

Make explicit which layer is responsible for movement, normalization, validation, governance, and workflow orchestration.

Instrument the workflow

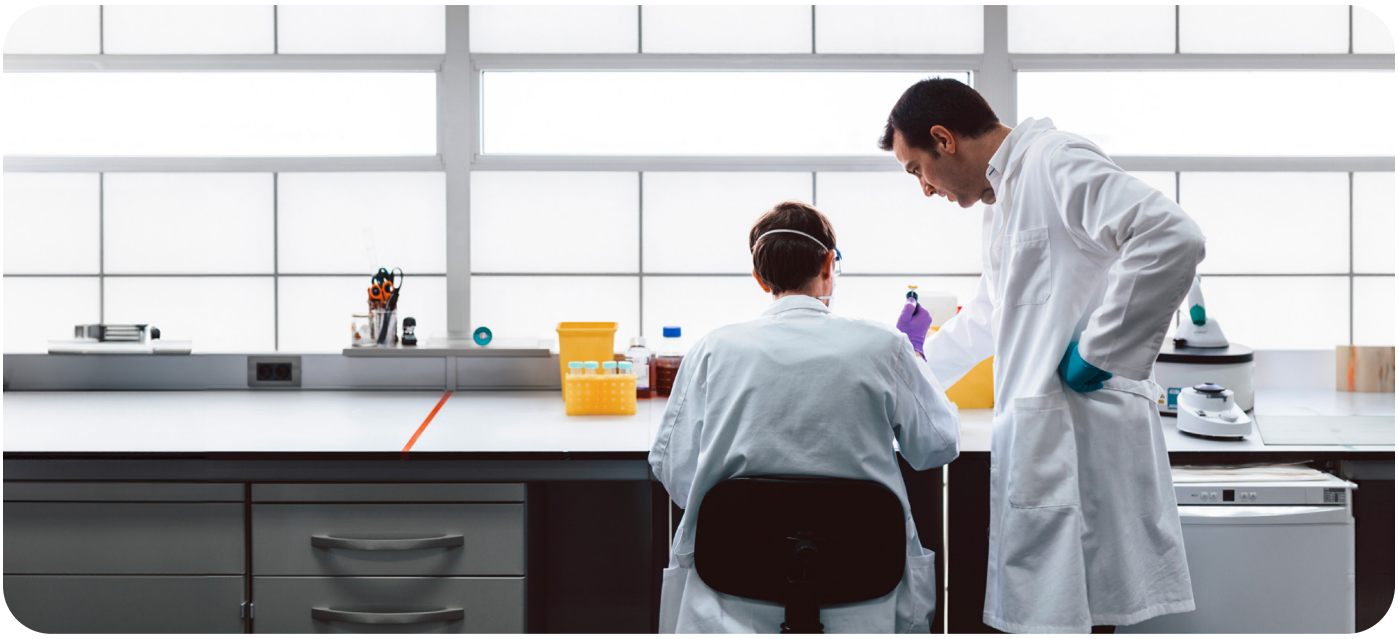
Measure technical and operational performance: availability, latency, data quality, exception rate, manual touches, cycle time, and outcome completion.

Design exception handling before scale

A happy path is not an operating model. Define how missing information, partner failures, ambiguous matches, and quality issues are surfaced and resolved.

Turn reusable capabilities into shared services

Package validation, terminology, identity, partner onboarding, provenance, monitoring, and orchestration patterns as shared services that make the next use case faster.



Building operational interoperability across the enterprise

Operational interoperability is not a single-product initiative. Healthcare organizations rarely need to replace every established system, integration, or workflow to make progress. They need a practical way to build on what already works, close gaps, and add standards-based access where it creates value. Most importantly, they need to carry trusted information into the workflows that depend on it.

The starting point will vary. An organization may be responding to aging integration infrastructure, a regulatory FHIR requirement, an unreliable cross-system workflow, a data-quality challenge, or an analytics or AI initiative. In each case, the approach is similar: define the operational problem, determine which existing capabilities should remain in place, and add what is needed to make the workflow trustworthy, measurable, and repeatable.

A strong foundation should help an organization:



- Connect systems, standards, and partners across its technology environment
- Reuse common services and patterns across additional partners and use cases
- Route information into the right process and make exceptions visible
- Validate and normalize information so it is fit for the workflow that will use it
- Add FHIR-based access without disrupting established integrations that continue to deliver value
- Preserve identity, terminology, context, and provenance as data moves across systems
- Monitor technical performance and operational outcomes

The objective is not to force every exchange through one technology or deploy every capability at once. It is to begin with a meaningful operational need, build the smallest reliable foundation that addresses it, and make each use case that follows easier to support.

What this looks like in practice: Preparing data for AI

When healthcare data is reused for AI, a successful exchange is only the beginning. Organizations must be able to trace the data to its source, preserve its meaning and context, and govern how it can be used. Building these capabilities into interoperability efforts today can support more responsible use of AI tomorrow.



What leaders should measure

DIMENSION	ILLUSTRATIVE MEASURES	REPRESENTATIVE CAPABILITIES
Connection	Availability, successful authentication, partner onboarding time, certificate/configuration incidents	Clinical workflows, administrative automation, analytics, population health, digital ecosystem services, AI
Data trust	Completeness, validation failures, unmapped terminology, identity match confidence, provenance coverage	FHIR resources, APIs, partner access, security, authorization
Workflow	Exception rate, manual touches, cycle time, queue age, completion rate	Validation, terminology, identity, provenance, data quality, governance
Scale	Reusable component adoption, partner-specific customizations, change failure rate, operational effort per connection	Routing, transformation, messaging, documents, events, workflow orchestration, monitoring
Outcome	Decision turnaround, administrative effort, quality performance, clinician/patient friction, analytics or AI reliability	Whether the interoperability investment matters

The same capabilities provide a framework for measurement. Technical metrics show whether information moved successfully. Data, workflow, scale, and outcome measures show whether the exchange produced operational value.

Conclusion: The endpoint is the beginning

Healthcare should recognize how much interoperability has advanced without mistaking progress for completion. The industry has built mature standards, connected previously isolated systems, expanded API access, and created more effective mechanisms for electronic exchange. Those accomplishments matter. They have also moved the challenge upstream.

The next generation of interoperability will be defined less by whether data can cross a boundary and more by what happens after it does.

The real measure of success is whether the receiving organization can trust the information, preserve its clinical and operational context, and route it into the right workflow. It must also be able to manage exceptions, reuse the capability across additional partners and use cases, and ultimately demonstrate a measurable outcome.

An API going live should therefore not be treated as the end of an interoperability initiative. It should trigger the next set of operational questions.

References

1. Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP/ONC). “Hospital Use of APIs to Enable Data Sharing between EHRs and Third-Party Technology.” Data Brief No. 81, February 2026. https://healthit.gov/data/data-briefs/hospital-use-of-apis-to-enable-data-sharing-between-ehrs-and-third-party-technology/

2. HL7 International. “FHIR Overview,” FHIR Release 5 (v5.0.0). https://hl7.org/fhir/overview.html

3. National Institute of Standards and Technology. “Artificial Intelligence Risk Management Framework (AI RMF 1.0).” NIST AI 100-1, January 2023. https://doi.org/10.6028/NIST.AI.100-1

4. National Institute of Standards and Technology. “Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile.” NIST AI 600-1, July 2024; updated April 2026. https://doi.org/10.6028/NIST.AI.600-1

Five questions to ask after the API goes live:

1. Can the right organizations and applications reliably discover, authenticate to, and maintain the connection?
Connectivity has to remain operational over time as endpoints, certificates, configurations, policies, and partner relationships change.

2. Is the data complete, consistent, in context, and fit for the workflow that will consume it?
Syntactic validity alone does not establish that the information is trustworthy enough for a clinical, administrative, analytical, or operational decision.

3. Can we trace where the information came from and what transformations occurred?
Provenance, lineage, normalization, and transformation history become increasingly important as data is reused beyond the workflow in which it originated.

4. Does the data enter a defined workflow with accountable owners and explicit exception handling?
Information creates value only when it reaches the appropriate process, person, service, or automated decision point and when the organization knows what happens when something goes wrong.

5. Can we prove the operational outcome and repeat the pattern for the next partner or use case?
Mature interoperability should make subsequent use cases easier to deliver rather than creating another custom integration project each time.

These questions become even more consequential as healthcare expands its use of artificial intelligence. AI models can accelerate analysis, automate tasks, identify patterns, and create new forms of decision support, but they do not remove the need for disciplined data engineering, governance, provenance, and operational control. They raise the stakes on weaknesses in those areas because data that is incomplete, stripped of its context, or poorly governed can now shape decisions at greater speed and scale.

The strategic objective, therefore, is not simply more interfaces, more endpoints, or more FHIR resources. It is a reusable interoperability foundation that connects systems, builds trust, preserves context, turns data into action, and supports accountable workflows, making each use case that follows easier to deliver. That is the shift from **moving healthcare data** to **making it useful**.





About Infor

Infor is a global leader in business cloud software products for companies in industry-specific markets. Infor builds complete industry suites in the cloud and efficiently deploys technology that puts the user experience first, leverages data science, and integrates easily into existing systems. Over 67,000 organizations worldwide rely on Infor to help overcome market disruptions and achieve business-wide digital transformation.

infor.com

Explore your path to operational interoperability

LEARN MORE

Copyright © 2026 Infor. All rights reserved. The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All other trademarks listed herein are the property of their respective owners.

WP-EN-0926-86akjxave-1