medinous

HOSPITAL LEADERSHIP GUIDE

The Hospital Cybersecurity Readiness Guide

10 questions to ask before choosing an HMS or digital-health platform.

A practical guide for hospital leadership, CIOs and healthcare IT teams – designed to assess access, traceability, resilience, integration risk and partner readiness.



Cybersecurity is patient care. Built for secure, connected hospitals.

INSIDE THIS GUIDE

01 Who can access patient data? 03

02 Can every critical action be traced? 04

03 How is sensitive data protected? 05

04 How secure are your integrations? 06

05 Can care continue during a disruption? 07

06 How strong is backup and recovery? 08

07 How are third parties controlled? 09

08 Can security scale across the enterprise? 10

09 Are privacy and compliance built in? 11

10 How prepared is your technology partner? 12

THE LEADERSHIP CONTEXT

medinous

Cybersecurity Is Where Patient Safety, Operations and Trust Meet.

Hospitals depend on connected systems for clinical documentation, diagnostics, medication, billing, insurance and patient engagement. As those systems become more connected, cybersecurity becomes closely tied to continuity of care and operational resilience.

PROTECT
Patient data

CONTINUE
Clinical operations

TRUST
Connected care

✓ Use this guide as a practical discussion tool when evaluating an HMS or digital-health platform.



01
OF 10

ACCESS CONTROL

01. Who Can Access Patient Data?

Not every user needs access to every part of the patient record. A secure HMS should make access reflect each person's role, responsibilities and care context.

ASK YOURSELF

- [ ] Is access defined by role?
- [ ] Can permissions be limited by function?
- [ ] Are privileged users controlled separately?

LOOK FOR

- ✓ Role-based access
- ✓ Least-privilege controls
- ✓ Strong authentication

WHY IT MATTERS

Strong access controls reduce unnecessary exposure while helping care teams reach the information they need.

> **"Access should follow responsibility - not convenience.**

AUDITABILITY

02. Can Every Critical Action Be Traced?

Hospitals generate thousands of digital interactions every day. When records are viewed, changed or shared, teams need to know who did what and when.

ASK YOURSELF

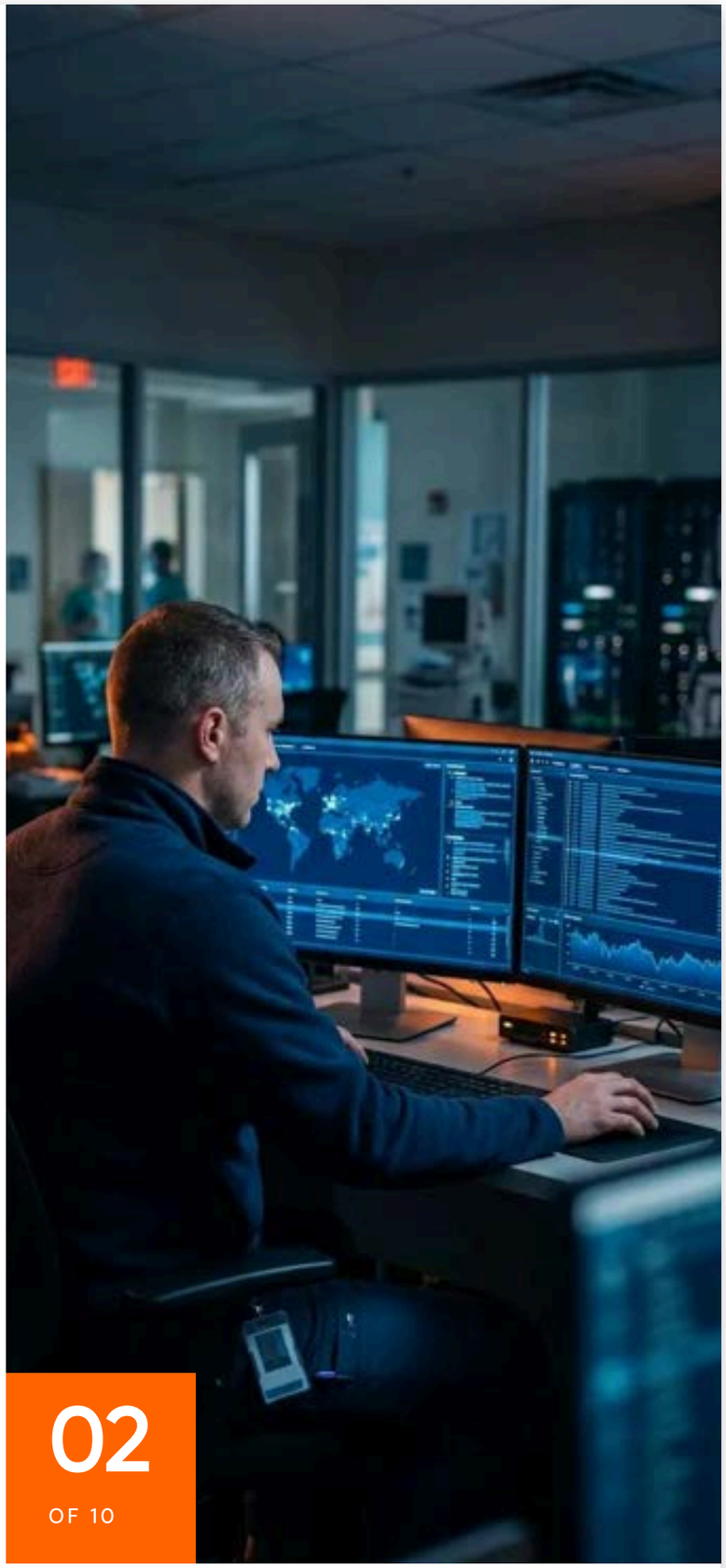
- [ ] Can record access be tracked?
- [ ] Can changes be traced to a user?
- [ ] Can unusual activity be investigated?

LOOK FOR

- ✓ Audit trails
- ✓ Access logs
- ✓ Activity monitoring

WHY IT MATTERS

Clear auditability supports accountability, governance and faster investigation when something unexpected occurs.



> **"If an important action happens in the system, there should be a way to trace it.**

02 OF 10



03
OF 10

DATA PROTECTION

03. How Is Sensitive Data Protected?

Patient information moves across departments, facilities and applications. Security therefore has to extend across the entire data journey, not only one screen or database.

ASK YOURSELF

- [ ] Is data protected while stored?
- [ ] Is it secure while moving between systems?
- [ ] Can downloads and exports be controlled?

LOOK FOR

- ✓ Encryption
- ✓ Secure data exchange
- ✓ Data governance

WHY IT MATTERS

Protecting information throughout its lifecycle helps reduce exposure as data moves through the hospital ecosystem.

> "Patient information should be protected wherever it travels.

CONNECTED SYSTEMS

04. How Secure Are Your Integrations?

A modern hospital rarely operates on one system alone. Every interface – laboratory, radiology, pharmacy, ERP, insurance, payments or patient apps – needs to be governed.

ASK YOURSELF

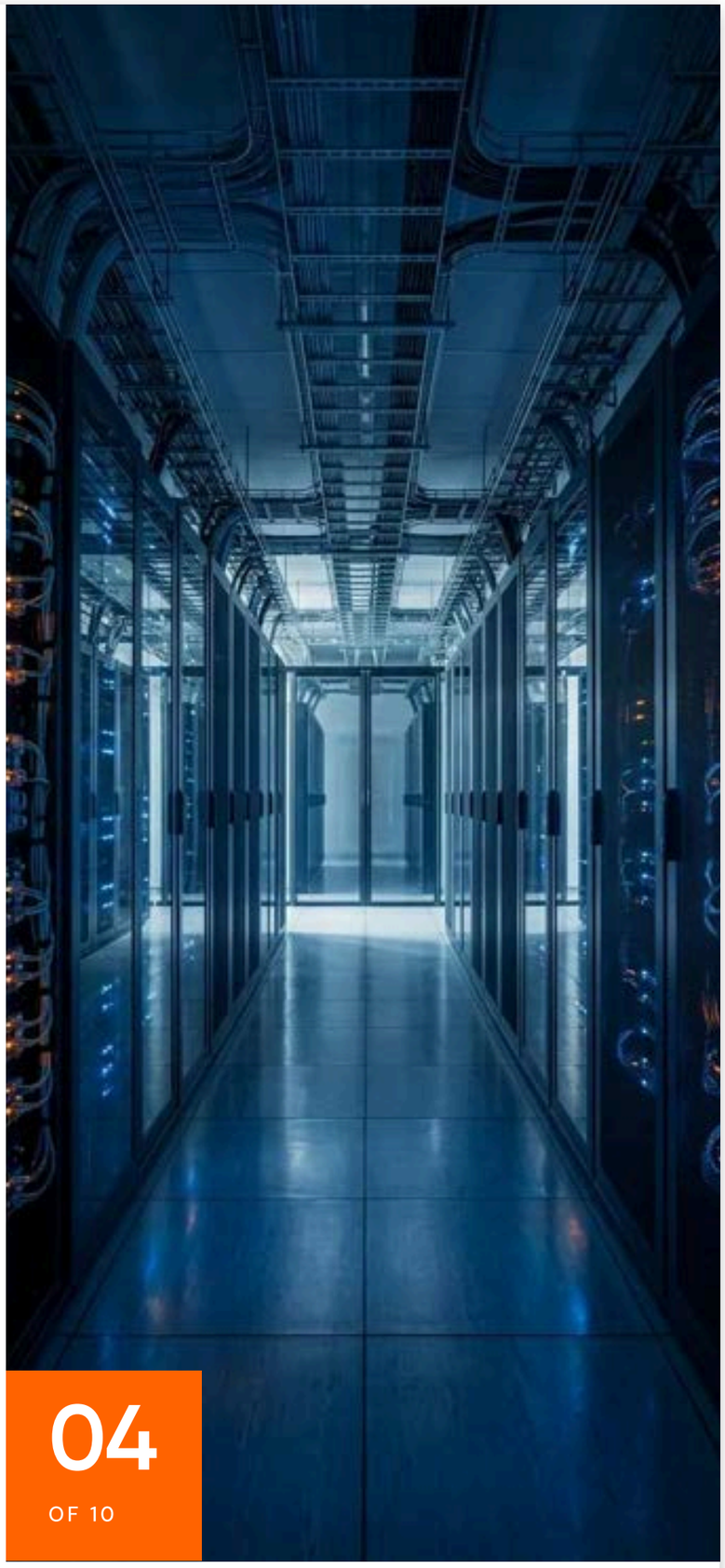
- [ ] Do we know every connected system?
- [ ] How are external systems authenticated?
- [ ] Are interfaces monitored?

LOOK FOR

- ✓ Secure APIs
- ✓ Authentication controls
- ✓ Integration monitoring

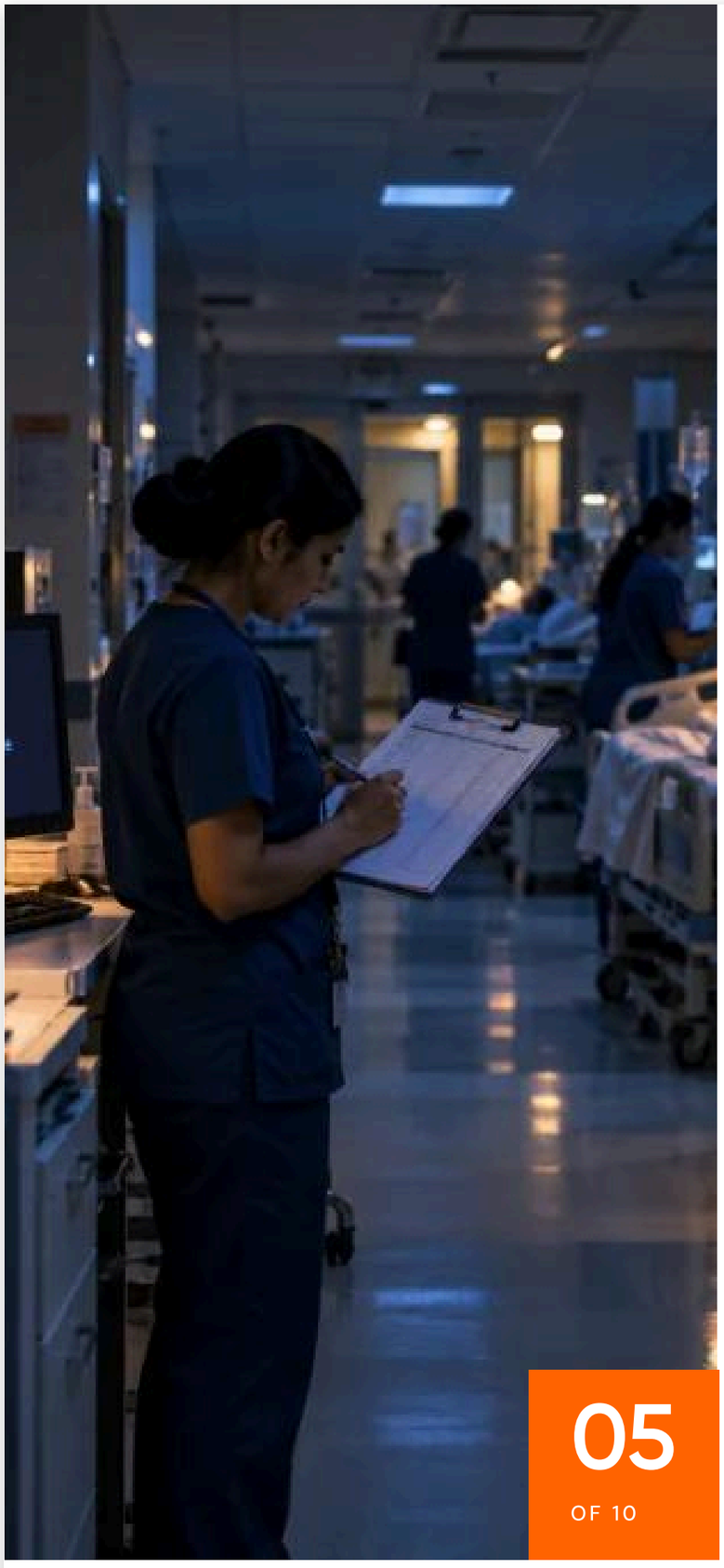
WHY IT MATTERS

Integrations create value, but every connection also expands the environment that needs to be secured.



> "Security gaps often sit between systems, not inside them.

04 OF 10



05
OF 10

OPERATIONAL RESILIENCE

05. Can Care Continue During a Disruption?

Cybersecurity is also about availability. If clinicians cannot reach records, results or medication information, a technology incident can quickly become an operational problem.

ASK YOURSELF

- [ ] Which workflows are mission-critical?
- [ ] What happens if the HMS is unavailable?
- [ ] How quickly can essential services recover?

LOOK FOR

- ✓ Business continuity
- ✓ Downtime workflows
- ✓ Recovery planning

WHY IT MATTERS

Resilience planning helps the hospital continue essential services while technology teams contain and recover from disruption.

> "Availability is part of continuity of care.

BACKUP & RECOVERY

06. How Strong Is Your Backup and Recovery Strategy?

Having a backup is not the same as being able to recover. Backups need to be protected, current and tested against realistic recovery scenarios.

ASK YOURSELF

- [ ] How often is critical data backed up?
- [ ] Are backups protected and isolated?
- [ ] When was recovery last tested?

LOOK FOR

- ✓ Secure backups
- ✓ Recovery testing
- ✓ RTO / RPO

WHY IT MATTERS

A tested recovery strategy reduces uncertainty and helps restore priority systems and data in a controlled way.

> "The real question is not "Do we have backups?" but "Can we recover?"



06
OF 10



07
OF 10

THIRD-PARTY RISK

07. How Are Third Parties and Vendors Controlled?

Cloud providers, integration partners and service vendors can extend access beyond the hospital itself. Their access needs the same discipline as internal access.

ASK YOURSELF

- [ ] Which vendors can access systems?
- [ ] What information can they access?
- [ ] How is access removed when no longer needed?

LOOK FOR

- ✓ Vendor assessments
- ✓ Controlled remote access
- ✓ Offboarding procedures

WHY IT MATTERS

Third-party governance gives hospitals visibility and control over risk beyond their own organization.

> **"Your security perimeter includes your partners.**

ENTERPRISE SCALE

08. Can Security Scale Across the Enterprise?

A healthcare organization may grow from one hospital into a network of hospitals, clinics, pharmacies and diagnostic centers. Security should scale with that growth.

ASK YOURSELF

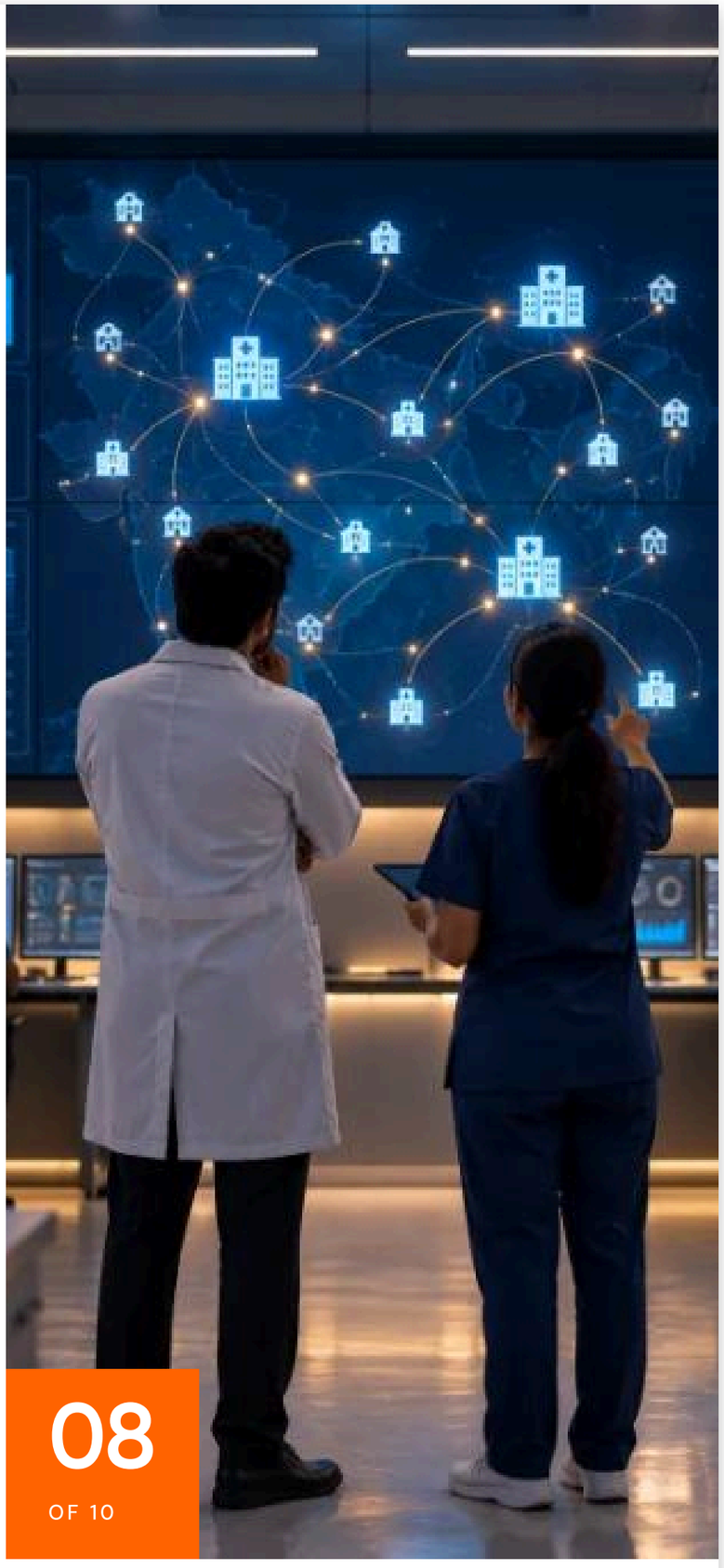
- [ ] Can policies work across facilities?
- [ ] Can access be managed centrally?
- [ ] Is activity visible enterprise-wide?

LOOK FOR

- ✓ Central administration
- ✓ Standardized policies
- ✓ Enterprise visibility

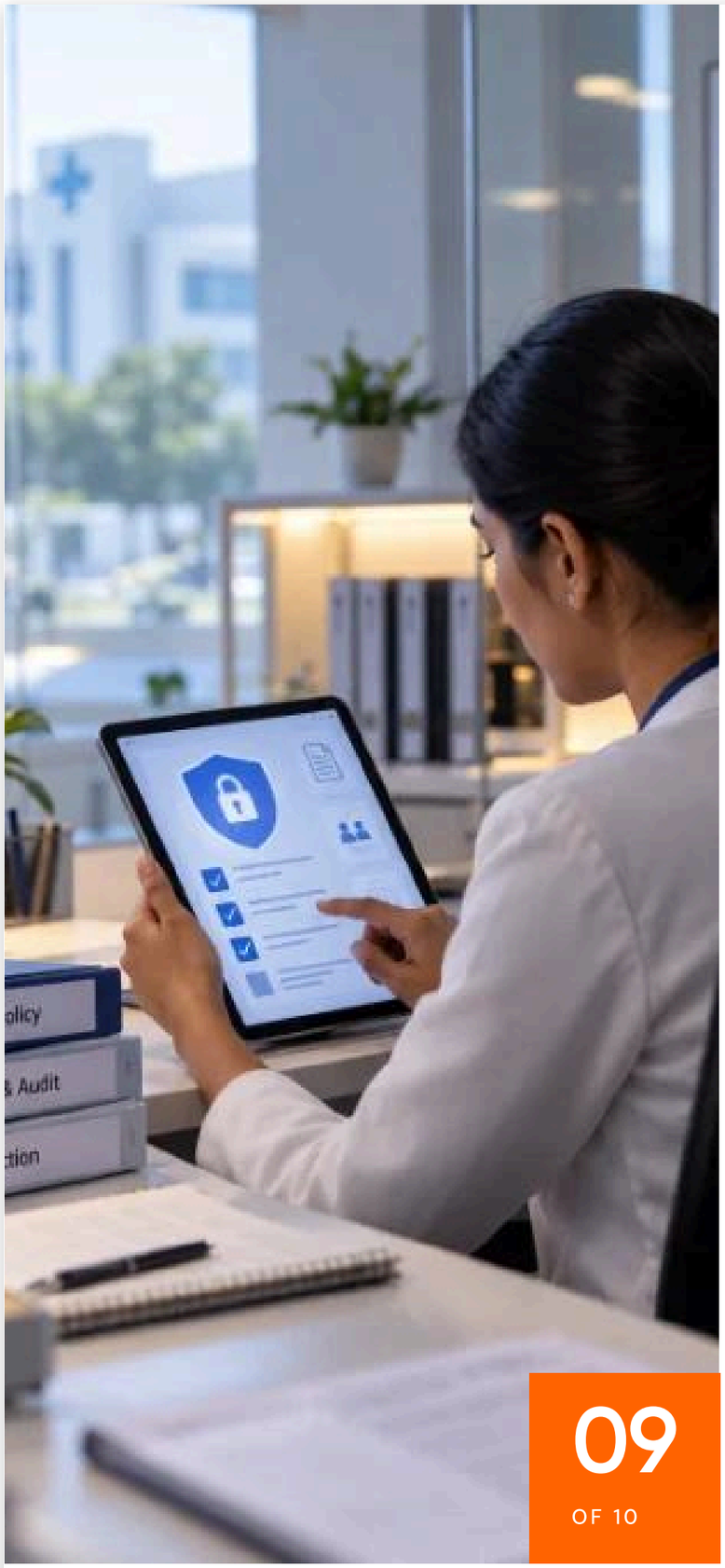
WHY IT MATTERS

A scalable security model helps growth without creating fragmented controls or new blind spots.



> "Growth should not make security harder to manage.

08 OF 10



09
OF 10

PRIVACY & COMPLIANCE

09. Are Privacy and Compliance Built Into the Platform?

Healthcare organizations face increasingly demanding privacy and data-governance requirements. Technology should help operationalize those obligations rather than rely on manual workarounds.

ASK YOURSELF

- [ ] Do we know where sensitive data is stored?
- [ ] Can access and retention be managed?
- [ ] Can audit records be produced when needed?

LOOK FOR

- ✓ Privacy by design
- ✓ Data governance
- ✓ Auditability

WHY IT MATTERS

Embedding privacy controls into the digital environment makes compliance easier to manage and demonstrate.

> "Compliance should be supported by the system - not by workarounds.

PARTNER READINESS

10. How Prepared Is Your Technology Partner?

Cybersecurity does not stop when the HMS goes live. Systems change, new integrations are added and vulnerabilities emerge over time.

ASK YOURSELF

- [ ] How are vulnerabilities managed?
- [ ] How are updates delivered?
- [ ] What happens during an incident?

LOOK FOR

- ✓ Patch management
- ✓ Incident response
- ✓ Ongoing governance

WHY IT MATTERS

A mature technology partner should be able to explain how security is managed throughout the platform lifecycle.



10
OF 10

> "Security is an ongoing discipline, not a one-time implementation task.

QUICK READINESS CHECK

Where Does Your Hospital Need a Closer Review?

Mark each area as Strong, Needs Review or Not Sure. The objective is not a perfect score – it is identifying where uncertainty remains.

		Strong	Needs Review	Not Sure
01	Access control	☐	☐	☐
02	Auditability	☐	☐	☐
03	Data protection	☐	☐	☐
04	Integration security	☐	☐	☐
05	Business continuity	☐	☐	☐
06	Backup & recovery	☐	☐	☐
07	Third-party security	☐	☐	☐
08	Enterprise scalability	☐	☐	☐
09	Privacy & compliance	☐	☐	☐
10	Technology partner readiness	☐	☐	☐

FROM CHECKLIST TO ACTION

Is Security Built Into Your Digital Hospital – Or Added After The Fact?

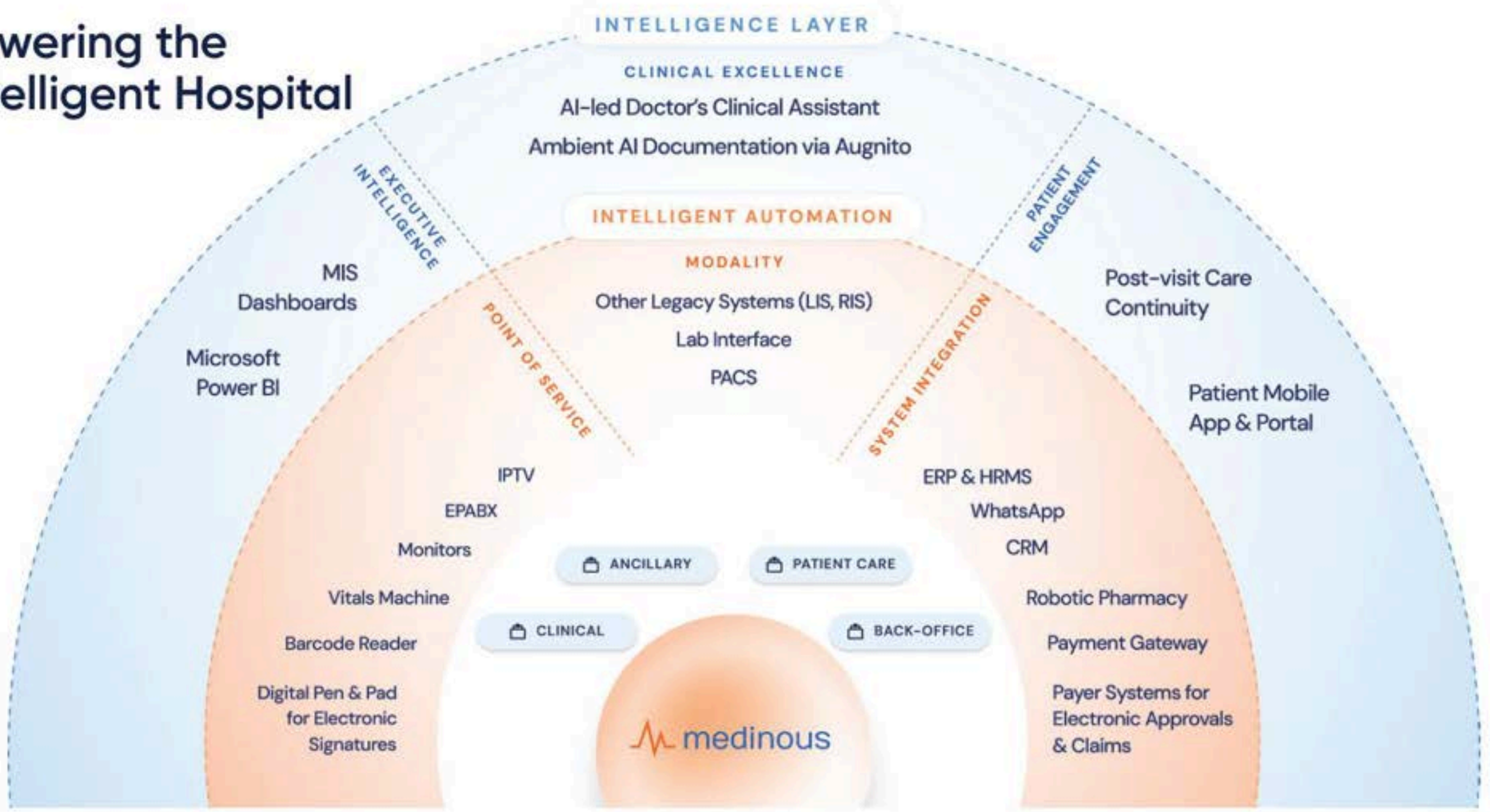
Use the checklist as a leadership conversation starter. The value is knowing where access, visibility, resilience or partner controls need attention next.

1. **MAP**
   Systems, users, integrations and data flows.
2. **PRIORITIZE**
   Critical clinical and operational workflows.
3. **CLOSE GAPS**
   Start where risk and uncertainty are highest.
4. **REVIEW**
   Reassess controls as technology and threats change.

Cybersecurity is patient care.

PLATFORM OVERVIEW

Powering the Intelligent Hospital



ARCHITECTURE LENS

Three questions before adding another AI layer.

1. **Connected to the record**
   Does it work from the longitudinal record rather than aseparate data copy?

2. **Governed by the HMS**
   Does it inherit identity, permissions, confidentiality andaudit controls?

3. **Useful in the moment**
   Does it remove retrieval steps inside the physician workflow?

MEDINOUS AT A GLANCE

One Connected Platform For The Clinical Workflow

Medinous brings hospital and clinic workflows onto an integrated platform spanning core clinical, specialty EMR, ancillary, patient-care and back-office functions - with AI-enabled Clinical workflows embedded where relevant.

10+ Countries
Presence

20,000+
Patients served daily

100,000+
Daily transactions

Ready to apply this to your clinical workflow?

Assess where information retrieval creates friction - and where AI can remove it safely. Start with one high-value clinical moment, then measure what changes.

Request a Demo



Tip: A next-generation HMS measures both cost and outcome—giving finance leaders the data to succeed in value-based reimbursement models.