Intraprise HEALTH
A Health Catalyst Company

Becoming OCR-compliant

Performing a Security Risk Assessments for MEDITECH Hospitals

HIPAA One™

Top 10 Security Risks

1. Control of PHI Can be Lost
- Control and visibility can be lost when you allow BYOD, removable media, ePHI downloads/exports stored on local devices

2. On Premise Vulnerability/Patch Management
- Keeping up with important Windows and MEDITECH updates
- Patching cadence, monitoring MEDITECH advisories

3. Auditing of Staff Activity
- Procedures to ensure regular activity reviews of ePHI access by staff
- Admin Privileges

4. Automated Emails
- Hospital hosted email system sending automated messages from MEDITECH
- Automated shift change Nursing emails which list patients and diagnoses

5. Integrations
- External EHRs/apps/devices, HL7, APIs, proper encryption of data feeds, etc.

6. REST API Infrastructure
- Secure REST API Infrastructure utilized for third party vendor software access to patient data
- Verification and security of patient portals

7. Encryption of Data in Motion [6.x, Patient Portal, Expanse Web Servers]
- Ensure proper TLS implementation between servers and end user devices

8. On Premise Backup/Restore
- Vetted backup solutions, integrity, encryption, Meditech-developed backup routine to validate backup and restores tests, and validate incident response procedures.

9. Insecure SMB Shares [On Premise; MAGIC, C/S, some 6.x]
- ANP for Scanning and Archiving, etc.

10. Signed Executables
- ANP for Scanning and Archiving, etc.

MEDITECH-based Security Risk Assessment

Performing a Security Risk Assessment (SRA) for a hospital's enterprise EHR, particularly those using legacy MEDITECH platforms, is crucial given the vast amounts of sensitive data they handle.

Whether hosted on-premise or in a hybrid private cloud, the MEDITECH platform is at a higher risk of data breaches, corruption, and ransomware attaks due to outdated infrastructure and configuration settings.

Is your Scanning and Archiving solution still using SMB shares?

Does your Consumer Health Portal implement patient identity in a secure manner?

How are you securing your Expanse Virtual Care?

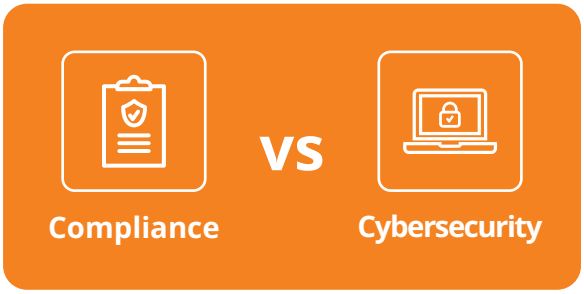
Consider the numerous integration point within your facility. Medical devices, external systems, and applications from multiple EHR vendors. These solutions communicate back and forth, but not always securely.

Key Risk Management Challenges

A few key common challenges that affect a majority of health systems are detailed below.

1. **Lack of Resources –** Health systems face limited security resources managing HIPAA compliance and cybersecurity. CIOs and CISOs often acknowledge staff and budget shortfalls, leaving them vulnerable to threats and breaches.

2. **Compliance vs Cybersecurity –** HIPAA compliance is legally required, and cybersecurity is crucial for effective risk management. However, the annual HIPAA assessment consumes significant staff time and budget, limiting resources for broader cybersecurity needs.



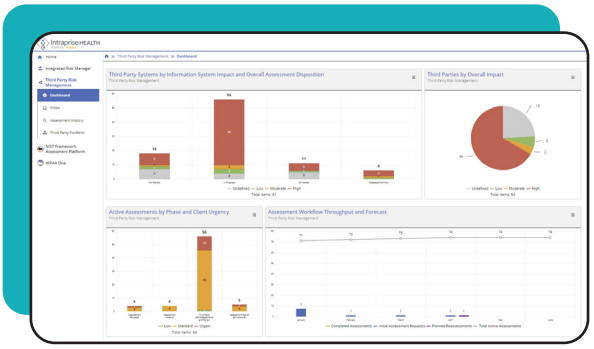
3. **Minimal YoY Leverage –** Using static questions and checklists for annual security assessments despite little change in responses and evidence year over year is inefficient.

4. **Lack of Enterprise-wide Coverage –** Traditional assessments often fail to capture enterprise-wide risks across all hospital locations, practices, and remote sites due to cost and resource constraints. Achieving a comprehensive view of all gaps and risks becomes challenging due to the diverse sources of risk.

Product Spotlight

Achieve a unified risk view with BluePrint Protect™ Integrated Risk Management Platform

Seamlessly import assessment risks and metrics from various sources, including HIPAA One and NIST CSF, for comprehensive enterprise risk management.



5. **Cyber Insurance Premiums/Coverage –** Insurance carriers often raise coverage requirements and premiums for organizations deemed to have insufficient "cyber maturity," increasing pressure to maintain reasonable premiums or demonstrate a highly effective cybersecurity program to retain coverage.

6. **Alignment Challenges with Boards and Executives –** Security leaders need more clear insight to engage with Boards and Executives. Meaningful risk management discussions are difficult without tools for performance trends, high-risk identification, and ROI demonstration.

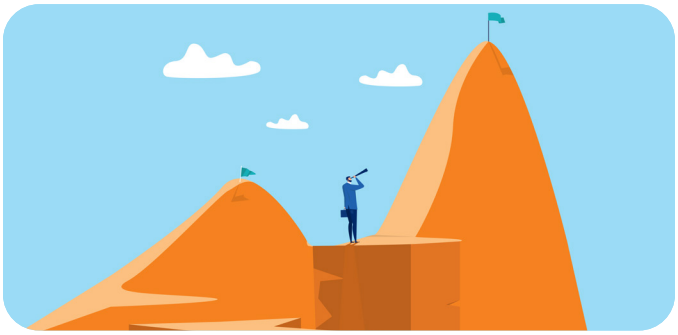
HIPAA One™ Enterprise:
SaaS-based assessment, remediation and OCR-readiness solution

No more juggling spreadsheets and PDFs!

- ✓ Pre-configured questions assess compliance with HIPAA Security standards (45 CFR 164.302-316)
- ✓ Remediation Management module
- ✓ OCR "Evidence Book" - Action History feature
- ✓ Auto-calculated CVSS risk ratings
- ✓ Compliance Dashboards
- ✓ Auto generated Report of Findings – technical, executive and custom options
- ✓ Downloadable Policy and Procedure library
- ✓ Meaningful Use/MIPS compliant reports
- ✓ HIPAA Safeguards mapped to **NIST SP800-53**

Leverage Efficiency Gains

- **Reusable Scope** – One-click download the previous assessment's scope and configuration of: ePHI systems, networks, servers, facilities, evidence, notes and assessment team members.
- **Dynamic Updates** – Linking parent (e.g., corporate) and child (e.g., provider practice) assessments keeps responses, policies, and remediation tasks synchronized across the organization.
- **One-to-Many Feature** – Push a controls template across your portfolio of ePHI systems and additional locations to enforce enterprise-wide security configuration standards.



"**Intraprise Health's HIPAA One Enterprise** software plus their industry leading cybersecurity services provide MEDITECH hospitals with a proven SaaS solution and EHR-specific security expertise required to perform an enterprise-wide SRA aligned with the latest OCR assessment standards.

It improves the maturity of your security program on a year-over-year basis while reducing stress for you and your security team."

Justin Armstrong, former MEDITECH Lead Security Architect

About Intraprise Health, a Health Catalyst Company

Intraprise Health, healthcare's leading compliance and cybersecurity organization, provides holistic visualization of your compliance and security posture. Our comprehensive services, backed by automation, rapidly integrate in native environments, yielding a comprehensive view of risk — spanning adherence to compliance frameworks, cybersecurity vulnerabilities, and third-party risk. Eliminate blind spots with Intraprise — the fifth HITRUST assessor since 2011.