HealthCatalyst

Frameworks in Action: Accelerating Healthcare Cybersecurity with Strategy, Speed & Compliance

Our Speakers

Scott Mattila
SVP, Product Strategy and Chief Security Officer

Health Catalyst

Ryan Patrick
VP of Adoption

HITRUST

Devin Shirley
Chief Information Security Officer

Arkansas

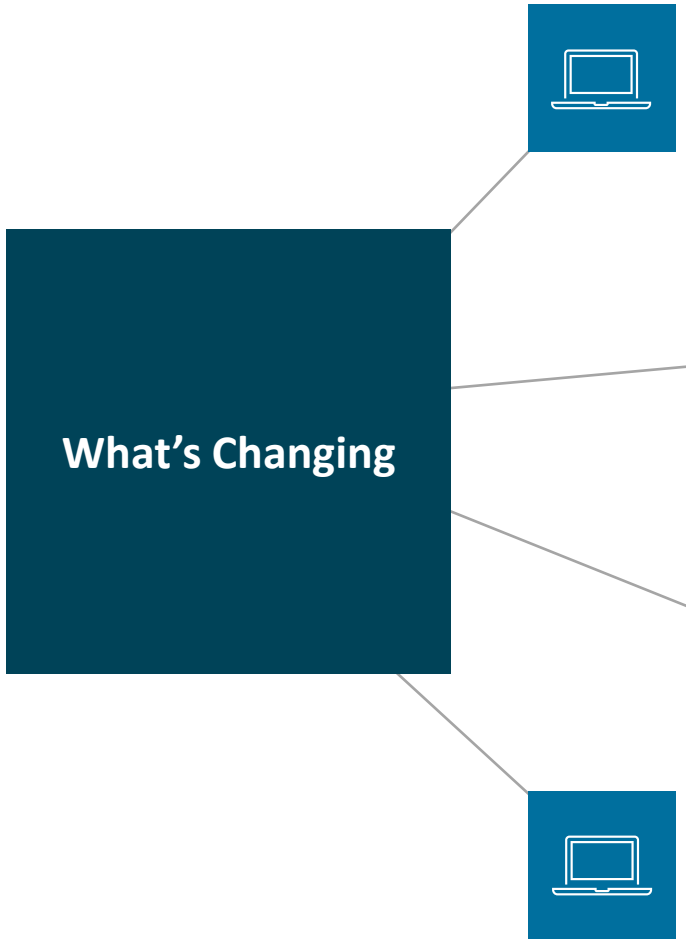
Agenda

- The Winds of Change in Regulation
- Frameworks for Measurable Impact
- Tips to Meet Strategic and Customer Demands
- Executives in Action, Driving Buy-in & Adoption
- HCAT Value Prop / Solution
- Q&A

The Latest Regulatory Changes Impacting Healthcare Security Programs

HealthCatalyst

Quick snapshot — what's changing (high level)



HHS/OCR's HIPAA Security Rule NPRM (Jan 6, 2025) — a major proposed overhaul to require more prescriptive, mandatory cybersecurity controls for covered entities and business associates (e.g., MFA, encryption, formalized IR planning, inventories, annual assessments, stronger vendor obligations). This is the single biggest federal change affecting how ePHI must be protected

Enforcement & scrutiny beyond HIPAA — OCR, FTC and state AGs are increasing enforcement on data-sharing, third-party disclosures, and deceptive privacy practices — especially for telehealth, apps, and digital health vendors. Expect bigger fines and public settlements.

Interoperability / Prior Authorization & data access rules (CMS) — rules forcing improved data exchange and prior auth automation continue to shape data flows and vendor/partner contracts. These push organizations to make data available while protecting it.

Regulatory focus on AI, analytics, and device/telehealth vendors — agencies (HHS/OCR, FTC, FDA) are increasingly flagging algorithmic transparency, claims scrutiny, and privacy requirements for analytics/AI in care. Expect guidance and enforcement around safe, explainable use of patient data.

HIPAA Headwinds and Strategic Impacts

The HIPAA NPRM — what it would *actually* require (key points)

Mandatory technical controls: MFA, encryption standards, network segmentation, and other formerly "addressable" safeguards may become *required*.

Stricter risk management: documented, recurring risk analyses; annual compliance audits; formal incident response and disaster recovery/backup plans.

Asset & workforce inventories + access controls: maintain inventories of hardware/software that store ePHI and stronger workforce access termination/attestation processes.

Stronger BA/vendor oversight: business associates will face tighter obligations (e.g., notification rules tied to contingency plan activation; more explicit contract requirements).

Increased documentation & auditability: more explicit recordkeeping and the expectation of evidence for compliance decisions.

Strategic impact for CIOs & CISOs

What changes in planning and priorities

From advisory to prescriptive execution — CIOs/CISOs can no longer treat many controls as optional; planning must budget, schedule and implement mandatory technical controls (MFA, encryption, backups, segmentation) across legacy and vendor stacks. HHS.gov+1

Vendor management becomes a core security control — procurement, contracting and vendor risk management teams need to be tightly integrated into security programs. Expect to rework BAA templates, SLAs, notification timelines, and audit rights. Reuters

Operationalizing evidence & audit readiness — compliance will require continuous evidence (asset inventories, logs, documented risk assessments, tabletop/exercises). Prepare for more frequent audits and enforcement inquiries. HHS.gov

Budget & staffing reallocation — costs for implementing and maintaining controls (technical and programmatic) will rise; CIOs must justify new spend for MFA, logging, backups, segmentation, and vendor oversight. HHS estimated substantial upfront costs in NPRM commentary. The Verge

Product & go-to-market changes for startups/vendors — startups that process ePHI must bake in these controls (or partner with compliant hosts) or risk losing customers. Vendors will be asked for stronger attestations and faster incident notification. cobalt.io+1

Security-by-design & privacy-by-default for digital health — AI, telehealth, and analytics vendors need privacy-preserving design, data minimization and stronger documentation of data use decisions to avoid FTC/HHS action. Reuters+1

How Leading Organizations are Operationalizing Frameworks for Measurable Impact

HealthCatalyst

Frameworks
Overload

Healthcare security programs must often comply with **multiple** frameworks simultaneously:

Challenge

Security leaders must map, reconcile, and show evidence across frameworks with *different control structures, languages, and audit expectations.*

Dynamic Risk Environment

New rules (like the **HIPAA NPRM**) and **ransomware-driven OCR enforcement** force programs to mature quickly. Yet many frameworks are static or outdated, leaving leaders unsure which benchmark is authoritative for regulators.

The Framework Fly-wheel

Measuring what matters…

How do I demonstrate program growth?

Should I be concerned that my maturity may decrease, based on the threat environment, tech stack change, or regulatory changes?

- Don’t boil the ocean, align your strategic imperatives, business goals, and outcomes to your measurement goals
- Measuring control maturity YoY
- Perfection in Cyber Security is not the goal, its continued growth, reduction in risk, and organizational readiness/response/adoption
- Drive accountability through team/organizational measures (top down/bottom up)

Tips to Align Security Efforts with Business Strategy and Customer Demands

HealthCatalyst

How do I better align my efforts to meet both customer and business needs?

Real-World Lessons on Gaining Executive Buy-in and Driving Adoption Across Teams

HealthCatalyst

Lessons Learned and Driving Adoption

The "human" side of cybersecurity strategy that separates a compliant paper program from one that actually sticks. Healthcare and SaaS leaders repeatedly encounter the same friction when trying to roll out frameworks like HITRUST, NIST, or ISO, or when tightening controls to meet customer contractual obligations.

Translate Cybersecurity into Business Risk and Trust

💡 *"Executives don't buy controls — they buy risk reduction, customer trust, and contract velocity."*

What works

Frame cybersecurity in business terms — tie each framework initiative to:

- Reduced likelihood of operational downtime or data breach fines.
- Faster **sales enablement** (ability to close contracts requiring security attestation).
- Improved **payer and partner trust** for HIPAA and HITRUST requirements.

Use short, visual **risk stories** rather than jargon-heavy control matrices.

- Example: "Without MFA across EHR access, one stolen password could expose 50,000 records — that's a $1.5M fine and six months of audit distraction."

Identify and create a **coalition of leaders** that can be your change drivers.

- From the janitor to the board, create a diverse team of change leaders.

Why Choose Intraprise Health & Blueprint Protect™

Your Partner in Healthcare Cybersecurity & Compliance Excellence

Why Intraprise Health

- 25+ years exclusively focused on healthcare data protection, privacy, and compliance.
- Deep alignment with HIPAA, HITRUST, NIST, and OCR standards.
- Acts as an extension of your CISO team—strategy, assessment, and execution
- Delivers measurable, ongoing risk reduction with proven healthcare expertise

Blueprint Protect™ – Continuous Cyber Resilience

- Unifies risk assessments, control management, and vendor oversight in one platform
- Automates Third-Party Engagement for evidence review and vendor engagement
- Provides real-time dashboards translating cyber risk into business insights
- Quick adoption, while standardizing your risk eco-system, to driving organizational accountability and risk transparency

Intraprise Health + Blueprint Protect™: From reactive compliance to proactive cyber resilience.

Questions?

Scott Mattila | SVP, Product Strategy and Chief Security Officer, Cybersecurity, Health Catalyst

Ryan Patrick | VP of Adoption, HITRUST

Devin Shirley | Chief Information Security Officer, Arkansas BlueCross BlueShield

Alora Martin | Webinar Program Manager

hcwebinars@healthcatalyst.com