Cybersecurity in Healthcare: Staying Informed and Protected

Joe Walker – Senior VP of Tech Services & Compliance at MyHealth Access Network

HIE Office Hours Decorum

- Panelists, please mute yourself when you are not actively speaking
- Attendees are automatically muted in the webinar
- To ask a question, please use the Q&A function
- The Presentation slide deck will be provided in an email following today's session
  - Today's session and past session presentations are all available on the MyHealth Website [Events– HIE Office Hours]

OKSHINE Program Reminders

OKSHINE Connection Fee Assistance Program

- Any organization that employs licensed Healthcare providers in the state of Oklahoma is eligible.
- Program covers all one-time fees from MyHealth to get providers connected to the state-designated HIE
  - Other related fees may be considered
- **Secure Connection Fee Assistance by applying at OKSHINE.gov**

SoonerSelect Provider Incentive Program

- Eligible providers can receive an estimated 28% increase in base fee schedule reimbursements for qualifying care and services
  - +18.5% base fee schedule increase for providers participating in SoonerSelect
  - +9.25% for Medicaid providers who participate in MyHealth, both sending data & utilizing the HIE
- **To apply, complete the MyHealth Application**

Introducing Our Speaker

Joe Walker, MSIE, CISSP

Senior VP of Tech Services & Compliance

MyHealth Access Network

- Founding member of MyHealth Access Network, Oklahoma’s non-profit Health Information Exchange (HIE)
- Over 15 years of experience in health IT, privacy, and security
- Chair of the Central Region for nationwide interoperability under the *Patient-Centered Data Home (PCDH)* initiative
- Leads community-wide committees on privacy, security, and operations management
- Experienced in policy development, data integrations, and identity matching systems
- Recognized for fostering collaboration across health care competitors to advance statewide data exchange

Why Cybersecurity Matters in Healthcare

Healthcare is a prime target for cybercrime

- Holds vast amounts of sensitive patient data
- Direct impact on patient safety and trust

The cost of a breach is high

- Financial: ransomware, fines, recovery expenses
- Reputational: loss of trust from patients & partners
- Operational: downtime disrupts care delivery

Cybersecurity is not just IT — it's patient care

- Protecting data protects patients
- Every staff member plays a role

The Current Threat & Vulnerability Landscape

Top Cyber Threats Facing Healthcare Today:

- **Phishing & Social Engineering** – deceptive emails, texts, or calls tricking staff into sharing access
- **Ransomware & Data Extortion** – locking systems until payment, often targeting hospitals & clinics
- **Insider Risks** – accidental disclosures or intentional misuse of access
- **Third-Party Vulnerabilities** – vendor systems or devices introducing risks
- **Internet of Medical Things (IoMT) Devices** – connected medical devices with limited security controls
- **Legacy Systems & Outdated Software** – older technologies that are difficult or costly to patch
- **Evolving Threats** – AI-driven attacks, more sophisticated malware, growing scale of incidents

Strengthening Defenses: Practical Steps

Organizational Best Practices

- Provide regular cybersecurity awareness training
- Develop & practice an incident response plan
- Review vendor security & contracts regularly
- Audit access logs and investigate unusual activity
- Apply the minimum necessary access standard data access

Everyday Actions for All Staff

- Participate in provided cybersecurity awareness training
- Use strong, unique passwords or passkeys + enable multi-factor authentication (MFA)
- Do not share credentials, including usernames or passwords
- Keep systems & software updated (patches close security holes)
- Think before you click: watch for phishing red flags (urgent requests, odd links, attachments)

MyHealth’s Role in Cybersecurity

Our Commitment to Data Security

- Compliance with HIPAA, HITECH, and federal/state regulations
- Continuous monitoring and auditing of systems
- Strong identity management & patient matching safeguards
- Maintains HITRUST r2 certification

Built-In Protections

- Encrypted data exchange across all connections
- Partnerships only with security-vetted vendors following best practices with continuous oversight
- Committees guiding policy and governance
- Can provide access to participant data during disaster recovery events

Collaboration & Support

- Ongoing provider training and resources
- Open, community-led governance to build trust
- Active role in nationwide interoperability initiatives (PCDH, CMS programs)

Takeaways

- Cybersecurity in health care = patient safety + trust
- Most breaches start with simple mistakes — awareness is your best defense
- Strong basics (MFA, updates, phishing awareness) go a long way
- MyHealth is your partner in secure, compliant data exchange

Example Resources for Cybersecurity in Healthcare

Federal & National Guidance

- **HHS 405(d) Program** – Practical cybersecurity practices for health care organizations, including the “Health Industry Cybersecurity Practices” (HICP) guide.
- **OCR (Office for Civil Rights) HIPAA Security Guidance** – Official HIPAA Security Rule guidance.
- **CISA (Cybersecurity & Infrastructure Security Agency)** – Alerts, best practices, and free tools for critical infrastructure, including health care.

Healthcare–Focused Organizations

- **Health-ISAC** – A trusted global community for sharing threat intelligence specific to health care.
- **NIST Cybersecurity Framework** – Widely used framework for assessing and improving cybersecurity readiness.
- **HIMSS Cybersecurity Resources** – Articles, toolkits, and reports on health IT and security.

Provider-Friendly Education

- **StaySafeOnline (National Cybersecurity Alliance)** – Consumer- and staff-friendly tips on online safety.
- **FTC Health App & Mobile Device Security** – For providers working with apps and patient-facing tech.
- **KnowBe4** – Security awareness training and phishing simulations
- **Oklahoma Foundation for Medical Quality** – Oklahoma’s healthcare consultants providing support and education

QUESTIONS?

THANK YOU!

Next Office Hours Session: 11/26/2025 at 12:15 PM

CONTACT

Joe Walker
Security@myhealthaccess.net

MyHealth Team
myhealth@myhealthaccess.net
marketing@myhealthaccess.net