Cybersecurity Primer for Healthcare Trustees

HTNYS

Healthcare Trustees of New York State

Why cybersecurity matters in healthcare

Healthcare organizations are prime targets for cyberattacks due to the high value of patient data and the critical nature of clinical operations. The consequences of a breach go beyond financial loss — a breach can disrupt patient care, damage brand reputation and result in regulatory penalties. Boards must ensure cybersecurity is central to their organization's clinical and operational strategy to protect patient care and outcomes.

Key risks and actions

1. Phishing and social engineering

RISK:

Phishing (fraudulent emails) and social engineering (manipulating staff into revealing sensitive information) remain the most common attack vectors. Attackers increasingly use sophisticated tactics including voice phishing ("vishing") and fake websites to trick employees into giving up credentials or clicking malicious links.

WHY IT MATTERS:

A single successful phishing attack can provide attackers with access to hospital systems and patient data and enable ransomware deployment.

ACTIONS FOR BOARDS:

- **Ensure regular, organization-wide cybersecurity awareness training, including simulated phishing exercises.**
- **Ask for metrics: What percentage of staff have completed training? What is the rate of phishing susceptibility?**
- **Confirm policies require reporting suspicious emails and there is a clear process for escalation.**

2. Ransomware

RISK:

Ransomware attacks encrypt hospital data and threaten to release sensitive information unless a ransom is paid. Healthcare is the most targeted sector, with attacks causing operational downtime, diversion of emergency care and significant financial loss.[1]

WHY IT MATTERS:

Downtime can disrupt patient care, delay procedures and erode public trust. Recovery costs and ransom payments can be substantial.

ACTIONS FOR BOARDS:

- **Require regular backups of critical systems and data, stored securely and tested for restoration.**
- **Ensure the hospital has a documented, tested incident response plan specifically for ransomware.**
- **Ask about the hospital's mean time to detect and respond to incidents.**

[1] TechTarget (April 8, 2026) FBI IC3: Healthcare sector leads in ransomware attacks. https://www.techtarget.com/healthtechsecurity/news/366641540/FBI-IC3-Healthcare-sector-leads-in-ransomware-attacks?_sp=a9e651cc-74ae-44a1-bcb0-31a6f6b5292a.1784208558818

3. Third-party and supply chain risk

RISK:

Many breaches originate with vendors or third-party partners who have access to hospital networks.[2] Despite this threat, many organizations lack a complete inventory of who has access.

WHY IT MATTERS:

A vulnerability in a vendor's system can be exploited to access hospital data, often bypassing internal controls.

ACTIONS FOR BOARDS:

- **Require a comprehensive inventory of all third parties with network access.**
- **Ensure contracts include cybersecurity requirements and regular audits.**
- **Ask when the last third-party risk assessment was performed and what high-risk findings were remediated.**

[2] American Hospital Association (January 2025) Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field. https://www.aha.org/system/files/media/file/2025/02/Change-Healthcare-Cyberattack-Underscores-Urgent-Need-to-Strengthen-Cyber-Preparedness.pdf

4. Insider threats

RISK:

Employees, contractors or partners may intentionally or accidentally compromise data. Such threats account for a significant portion of breaches.

WHY IT MATTERS:

Insiders often have legitimate access, making detection difficult. Incidents can result from negligence, lack of training or malicious intent.

ACTIONS FOR BOARDS:

- **Confirm access to sensitive data is limited to those who need it ("least privilege").**
- **Ensure monitoring tools are in place to detect unusual activity.**
- **Ask about the frequency and scope of internal audits.**

5. Internet of medical things and shadow IT

RISK:

Connected medical devices and systems outside central information technology control ("shadow IT") expand the attack surface. Many devices lack robust security controls.

WHY IT MATTERS:

Compromised devices can disrupt clinical operations or be used as entry points for broader attacks.

ACTIONS FOR BOARDS:

- **Require asset management policies that include all connected devices.**
- **Ask about vulnerability assessments and patching schedules for IoMT.**
- **Ensure network segmentation separates clinical, administrative and guest systems.**

6. Regulatory compliance and incident reporting

RISK:

Failure to comply with state and federal regulations (e.g., DOH, HIPAA) can result in penalties and increased scrutiny. Regulations require annual risk assessments, incident reporting within 72 hours and board-level oversight.

WHY IT MATTERS:

Non-compliance can lead to fines, loss of accreditation and reputational harm.

ACTIONS FOR BOARDS:

- **Ensure annual risk assessments are performed by qualified third parties.**
- **Confirm the board reviews and approves the cybersecurity program and risk assessment annually.**
- **Ask about the hospital's process for reporting incidents to regulators and lessons learned from past events.**

The board's role: Oversight and accountability

Boards do not need to be technical experts but must ensure:

- **Accountability:** There is a designated chief information security officer, even if part-time or contracted.
- **Culture of compliance:** Cybersecurity is prioritized and integrated into clinical and operational strategy.
- **Resource allocation:** The cybersecurity budget is adequate for staffing, tools and training.
- **Continuous improvement:** Policies, plans and training are regularly updated and tested.

RESOURCES

- HTNYS Board Responsibilities. https://htnys.org/resources/board_responsibilities
- NYSDOH Hospital Cybersecurity Requirements. https://www.health.ny.gov/facilities/hospital/cybersecurity
- Health Sector Coordinating Council, Cybersecurity Working Group. https://healthsectorcouncil.org

Healthcare Trustees
of New York State

HTNYS.org