Key Ways to Protect Patient Data from Emerging Cyber Threats

Iroquois Healthcare Association

October 15th, 2024

withum
ADVISORY TAX AUDIT

Meet Your Presenter

Edward Keck, Jr.
Partner, Market Leader,
Cyber and Information
Security Services

ekeck@withum.com

Learning Objectives

- ✓ Identify examples of recent cyber incidents and understand how they can materially impact your organization
- ✓ Recognize current cyber and information security trends impacting organizations and their patients
- ✓ Prepare to ensure the right cybersecurity programs and controls are in place

Cyber Breach Insights for 2024

- According to Health and Human Services, over 60 million records have been exposed in 2024 with the majority of these being the result of hacking/IT incidents.
- Change Healthcare's report to HHS only included 500 records. In reality, over 4 TB of data was exfiltrated representing PHI for millions of patients.

Cybersecurity Statistics for 2024

- 2024 has resulted in almost 500 reported breaches of PHI
  - Over 350 of these breaches were with Healthcare Providers
- Healthcare was not immune to the MoveIT vulnerability and subsequent data loss
  - Wisconsin Physicians Service Insurance notified Center for Medicaid & Medicare Service of breach due to MoveIT file transfer software

Why Are Healthcare Organizations Targeted?

TYPE OF DATA

HEALTH INSURANCE FRAUD

DRUG ABUSE AND TRADE

IDENTIFY THEFT

CREDIT CARD FRAUD

EMAIL DATABASES

Changing Threat Landscape

- Threat actors take advantage of opportunity.
- They can purchase tools, a commodity, reducing the cost of entry and skill sets.
- Ransomware as a Service (RaaS)
- Internet Facing Systems
- Synthetic Accounts
- Medical Devices - Operational Technology (OT) or Internet of Things (IoT)
- Supply Chain & Third-Party Service Providers
- Nation state activity continues to expand (China, Russia, Iran) impacting critical infrastructure.

2024 Cyber Breach Examples

withum
ADVISORY TAX AUDIT

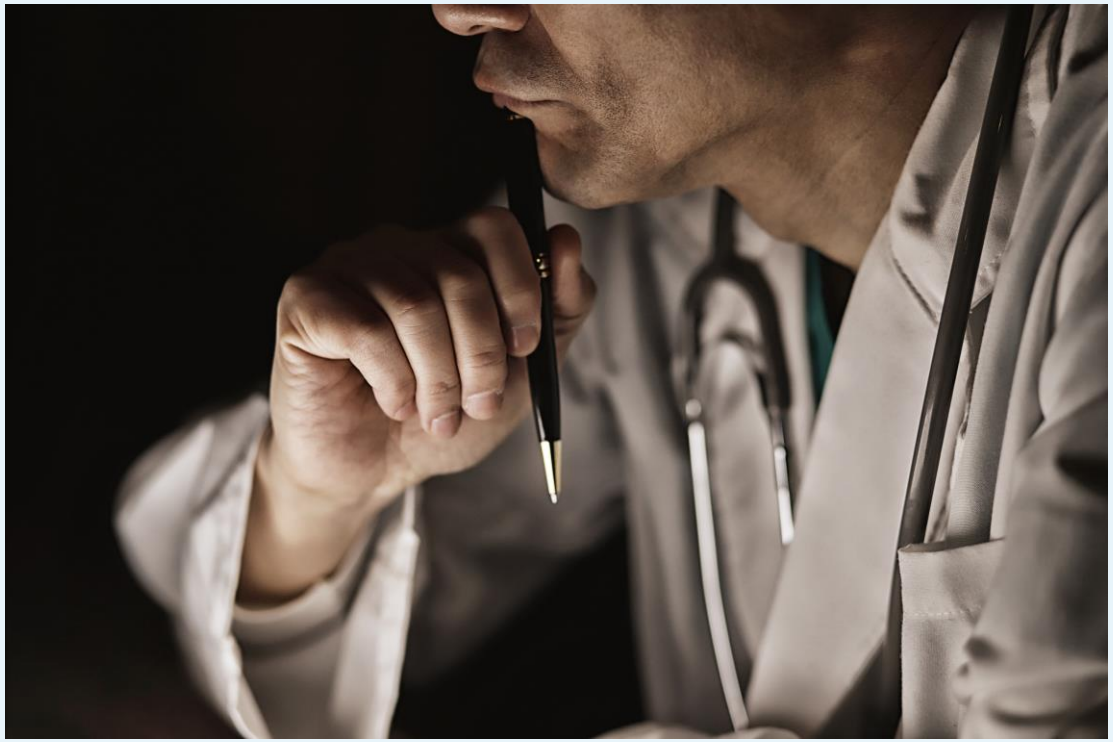
Significant Breaches

Change Healthcare

- Not just PHI data exfiltration
- Significant disruption to medical claims processing nationwide
- Impact on prescriptions as a processor

Ascension Healthcare

- Electronic medical records system impacted for a month
- Hospitals forced to divert ambulances
- Significant financial toll



Why Does The Healthcare Industry Struggle with Cybersecurity?

- HIPAA – Administrative, Technical and Physical Safeguards
- Cyber Hygiene
- Outdated Technology, Software & Patching
- Lack of adequate security controls in Medical Devices and Mobile Applications
- Lack of In-House Expertise
- Continuity Planning
- Third Party Risk Management
- Insufficient Cyber Training and Awareness amongst medical staff.
- Limited or No Risk Management

“If I have a cyber incident, what do I do?”

Follow your Incident response plan

Know who to call

Preserve evidence

Contain the breach

Incident response management

Investigate and fix your systems

Where Can I Begin?

- Cybersecurity Advisor to review your Cybersecurity Program
- Understand your Information Ecosystem
- Risk Assessment – Foundation of the Information Security Program
- Business Resiliency Planning
- Review of Critical Third - Party Vendors
- Cyber Insurance Review
- Retain Key Vendors for Incident Response
- Table-Top Exercise for Your Incident Response

Thank you! Questions?

Edward Keck, Jr.

ekeck@withum.com

withum
ADVISORY TAX AUDIT