HIPAAtrek

Privacy and Security Best Practices: Tales from the Field

May 2025

Meet the Speaker

Joe Wivoda

What is the Threat?

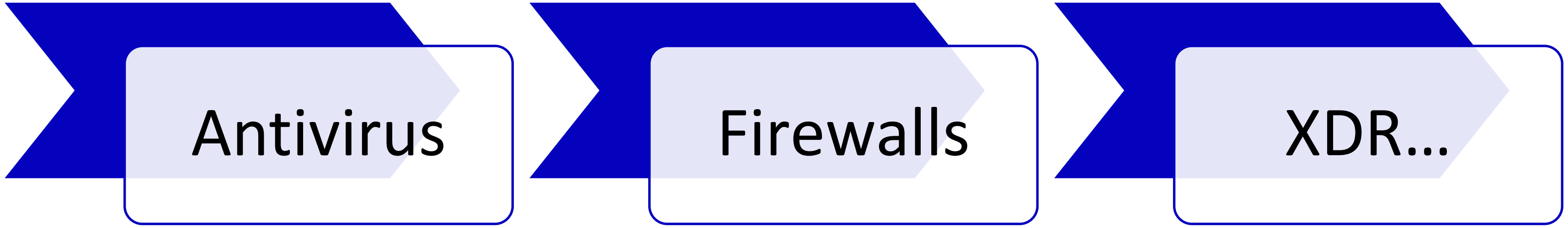
- According to HHS Office of Civil Rights (OCR), as of April 2025:
  - **537,156,883** patient names have been **REPORTED** to have been breached since tracking began (only includes breaches > 500 patients).
  - This **DOES NOT INCLUDE** breaches currently being investigated ≈ **331,000,000**!
  - 467,000,000 (87%) of those breaches are reported as having either hacking or other IT issue being a factor.

- Medical records are incredibly valuable!
  - **Credit Card Number**: < $5
  - **Social Security Number**: <$20
  - **Medical Record**: Between $100-$1,300

Downloaded 04/25/25 from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Evolution of Cyber Threats

- **1980s-1990s**—Viruses and firewall breaches
- **1990s-Early 2000s**—Worms, firewall/VPN breaches
- **2000s-2010s**—Advanced Persistent Threats (APT) and Social Engineering Attacks
- **2020s**—Ransomware with sophisticated social engineering and AI, Third-Party Exposure, state-sponsored attacks, infrastructure attacks



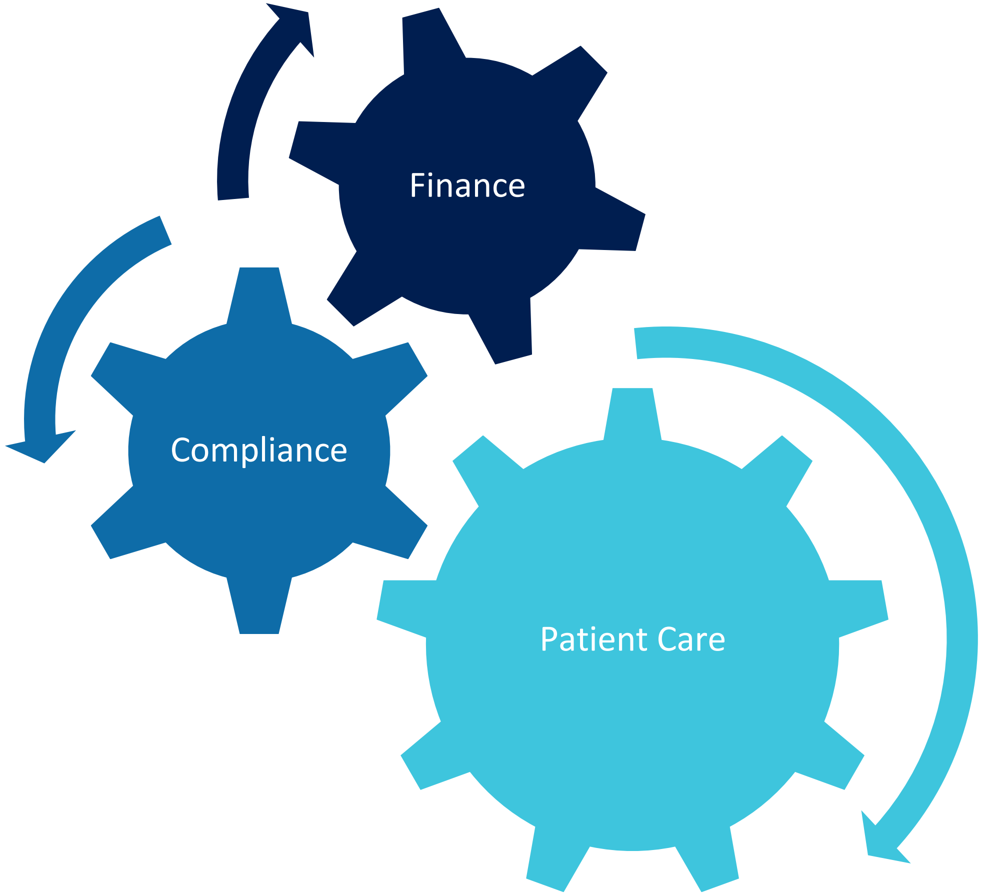
Antivirus

Firewalls

XDR…

Integrated Compliance

- Embed compliance into daily operations, not silos
- Compliance as a revenue protection strategy
- Transparency and common-sense risk management
- Use Get Out of the Office (“GOO”) to spot risks before they become violations
- Build compliance confidence across the organization



Compliance *IS* Risk Management

- Identify gaps and risks early
- Build a system-wide compliance process
- Recognize old update methods will fail
- Create a rollout plan for rapid regulatory changes
- Protect revenue, reduce risk, build confidence

Building a Cybersecurity Culture

- Cybersecurity is an Organizational Effort
- Hackers Use Social Engineering
- Rural & Small Healthcare Facilities Are Targets
- Sensitive Information Leaks Are Everywhere
- All Departments Play a Role
- Preparedness and Awareness are Key

Importance of Privacy & Security in Healthcare

- **Privacy and Security are Interdependent:**
  - **Privacy** protects patient PHI and controls access
  - **Security** safeguards PHI from unauthorized access, loss, or theft
- **You can't have privacy without security and vice versa:**
  - Weak security measures exposes PHI to unauthorized access, violating privacy.
  - Strong security is useless if PHI is shared improperly or without authorization.
- **Both are necessary:**
  - **Security** is the lock, and **Privacy** is the rule about who has the key.

Leadership's Role

Understand the **value** in compliance

Challenge simple solutions and silos

Ask questions and build awareness – Be visible!

Be aware of the various perspectives

Understand Risk Management and the SRA process

Security Risk Analysis

Foundation of your security and privacy program

📋 Key Components:

- Needs to be complete and thorough
- Vulnerability scanning of internal and external networks (websites, firewalls)
- Physical and facility security review and walkthrough
- Administrative controls assessment
- Technical controls evaluation
- Processes and practices involving security

📊 Risk Modeling:

- Model threats and vulnerabilities and their impact on risk
- Formula: **Risk = Threats x Vulnerabilities – Controls**

Ransomware Preparedness: Training and Detection

🔐 Ransomware Threats:

- Relies on social engineering and lack of awareness
- Third-party/supplier attacks increasingly common
- Cloud vendors must be part of response planning

🛡 Ransomware Readiness:

- Regular training and security reminders
- Tabletop exercises to simulate real incidents
- Include cloud vendors in planning scenarios
- Multi-factor authentication (MFA)
- Extended Detection and Response (EDX/XDR)
- Contingency and Incident Response Plans

Protecting Data: SRA’s Approach to Ransomware Prevention

📌 Scenario:

- SRA identified ransomware as a major threat and high risk

📋 Awareness and Planning:

- Education on ransomware/phishing
- Disaster recovery and contingency planning
- Breach Preparedness Assessment (BPA)/tabletop exercises
- Incorporated into Incident Command process

🔒 Technology and Detection:

- More complete technology inventory
- Phish testing
- Two-factor authentication
- Advanced threat detection

🛡️ **Results: THREE** thwarted ransomware attacks!

Securing PHI: The Get Out of the Office (GOO) Initiative

📌 Scenario:

- SRA identified PHI left visible on desks, in large boxes next to desks, and in the trash

🛑 Challenges:

- PHI left visible on desks, boxes, trash
- No shredding policy or leadership workstation review
- Shred bins in inconvenient locations

💡 Improvements:

- “Shred drawers” required for all PHI handlers
- Relocated shred bins to accessible spots
- Leadership actively reviews workstations

🏅 Impact:

- Activate GOO initiative ongoing
- Rewards program encourages compliance

Tabletop Exercises

- **Annual requirement** under Security Rule NPRM
- More than just **DRP** – tests full incident response
- Develop **scenarios** based on **identified risks**
- **Cross-department effort** with Incident Command training
- **Facilitator** needed to ask follow-up, probing **questions**
- **Scribe/notetaker** required, but must not participate
- Involve **clinical, facilities, admin, IT**, and other relevant staff

Strengthening Response: Effective Tabletop Exercises in Action

📌Scenario:

- Near-breach caused by disgruntled former employee

🔍 Findings:

- PHI security gaps
- Weaknesses in termination/offboarding
- Disaster recovery and contingency plan gaps
- Facility access issues

💡 Improvements:

- Process updates in HR, Maintenance, Nursing, Admin, IT, and more!

Planning for Breach Resilience

🔥 PREVENT (Avoid the Fire)

- Use sound IT security practices
- Maintain strong physical safeguards
- Monitor critical systems continuously
- Train staff for breach prevention

🚨 PLAN (Survive the Fire)

- Prepare for resilience (impact x likelihood)
- Identify key incident leaders
- Maintain offline-accessible critical asset lists
- Build flexible incident response plans
- Empower staff to act at top of license
- Practice through tabletop exercises

Fire drills don’t prevent fires—they prepare you to survive them. Your breach plan should too.

HIPAAtrek

Thank you for joining us!

Any questions?

Contact us:

info@hipaatrek.com

833.217.5400

hipaatrek.com/request-demo