

# Webinar Summary: Understanding IT & Cybersecurity for Healthcare Leaders

Presented by: Pat Hawn (Host) • Oscar Elmore (Solutions Engineer, IT Solutions) • Roxanne Rabich (Former Practice Administrator, IT Solutions) • Jess Bennett (Moderator) • Barbara Faupel (President-Elect, MGMA)

## Purpose of the Webinar

This session aimed to demystify IT and cybersecurity concepts for non-technical healthcare professionals—especially practice administrators, managers, and executives—so they can better communicate with internal or external IT teams and make informed decisions about their organization's technology infrastructure.

## Key Topics Covered

### ■ Cybersecurity Framework Using a Home Security Analogy

Oscar Elmore broke down cybersecurity into four layers: Prevent – Locking the front door (e.g., antivirus, firewall). Detect – Sensors and alarms (e.g., spam filters, EDR). Monitor – Surveillance and alerting (e.g., MDR, SOC). Respond – Taking action (e.g., MXDR, SIM tools). This analogy helped attendees visualize how layered security protects healthcare data and systems.

### ■ Importance of Multi-Factor Authentication (MFA)

MFA is a critical security measure, even if inconvenient. Authenticator apps are preferred over SMS due to phishing risks. MFA helps prevent unauthorized access, especially when passwords are reused across platforms.

### ■ Human Error & Cybersecurity

The weakest link in cybersecurity is often the end user. Real-world examples (e.g., spoofed emails, invoice fraud) illustrated how vigilance and training can prevent breaches. Encouragement to 'go old school' and verify suspicious requests via phone.

### ■ Role of IT Tools in Compliance & Insurance

Tools like SIM and SOC help meet HIPAA and cyber liability insurance requirements. Having these tools in place can reduce fines and aid in forensic investigations after a breach.

### ■ Bridging the Communication Gap Between IT and Healthcare Staff

Avoid jargon and acronyms; explain issues in terms of workflows and tools. Encourage staff to report issues early to prevent escalation. Leaders should foster a culture of open communication and proactive reporting.

### ■ Managing Up & Gaining Buy-In from Physicians

Use trusted relationships or bring in IT experts to help communicate the importance of policies. Frame security measures as mission-critical to protect patient data and organizational integrity.

### ■ When to Consider External IT Partners

Signs include overwhelmed internal staff, outdated hardware/software, slow issue resolution, and lack of strategic planning. External partners can complement internal teams by filling skill gaps and providing specialized support.

### ■ MGMA's Role & Resources

Offers education, certification, networking, and advocacy. Helps members stay informed and connected. Provides access to vetted vendors and peer support.

## Glossary of IT & Cybersecurity Terms

Term & Definition
<b>Antivirus</b> Software that detects and blocks known malware.
<b>Firewall</b> A device or software that filters incoming and outgoing network traffic.
<b>EDR (Endpoint Detection and Response)</b> Detects threats on devices and provides response capabilities.
<b>MDR (Managed Detection and Response)</b> Outsourced monitoring and response service for cybersecurity threats.
<b>MXDR (Managed Extended Detection and Response)</b> Adds monitoring for cloud-based applications and external systems.
<b>SOC (Security Operations Center)</b> A team or facility that monitors and analyzes security threats in real time.
<b>SIM (Security Information and Event Management)</b> Software that collects and analyzes log data for threat detection and compliance.
<b>MFA (Multi-Factor Authentication)</b> Security method requiring multiple forms of verification to access systems.
<b>HIPAA</b> U.S. law that mandates data privacy and security for medical information.
<b>Spoofing</b> A cyberattack where a malicious actor disguises communication to appear legitimate.
<b>Phishing</b> Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy source.

**VPN (Virtual Private Network)**

Encrypts internet traffic and masks user identity online.

**Help Desk**

IT support service that assists users with technical issues.

**MSP (Managed Service Provider)**

A third-party company that manages IT services for organizations.