CYBERSECURITY IN HEALTHCARE WORK GROUP

July 16

IOWA HOSPITAL ASSOCIATION

PROGRAM AGENDA

8:30 a.m. **Breakfast and Networking**

8:50 a.m. **Welcome**
Gary Davis, Vice President, Information Technology Operations and Security, Iowa Hospital Association, Des Moines

9 a.m. **AI + Cyber Insurance - Emerging Risk Trends in Artificial Intelligence**
Stephanie Snyder Frenier, Senior Vice President, Cyber Liability Practice and Cameron James, Area Vice President, Healthcare, Gallagher

Artificial intelligence is transforming organizations by driving efficiencies and boosting revenue. Although many have already adopted AI tools, it's crucial to consider the new exposures these technologies bring. This presentation will explore the emerging risks associated with AI use and how insurance policies cover "silent" AI risks. We will also delve into risk management strategies and frameworks to help your organization stay one step ahead.

Learning objectives:
- Consider risk management strategies to address AI risks
- Examine the National Institute of Standards and Technology and the International Organization for Standardization risk management frameworks
- Learn corporate uses of AI and risk considerations
- Understand how insurance policies cover "silent" AI risks

10 a.m. **Break and networking**

10:15 a.m. **Practice for the Test: Reverse-engineering the Office of Civil Rights' Ransomware Investigation Questions**
Alex Boyd, Shareholder, Polsinelli Law Firm

When a hospital or other HIPAA-covered entity reports a data breach, the U.S. Department of Health and Human Services' Office of Civil Rights is likely to investigate. Many organizations are unprepared when the office requests detailed evidence of the incident and the entity's underlying HIPAA compliance and cybersecurity program. By studying the office's questions in advance, organizations can better align internal policies, technical processes and incident response workflows with the Office of Civil Rights' expectations. This session will help healthcare leaders prepare for the scrutiny that can follow a ransomware event.

Learning objectives:
- Analyze real-world examples of cyber incidents – such as executive impersonation, payroll fraud and account takeovers – to understand how these attacks are executed and detected
- Apply practical strategies to strengthen cybersecurity posture, including improving monitoring capabilities, reducing organizational exposure, and protecting workforce identities and digital assets
- Identify emerging cybersecurity threats affecting healthcare organizations, including attacks targeting workforce identities, external exposure points and third-party vulnerabilities

11:15 a.m. **Why Network Segmentation Matters in Healthcare**
Jared Van Wyk, Director of Network Professional Services and Bryan Stanford, Sales Executive, Carrier Access IT

Network segmentation is one of the most practical defenses that hospitals can invest in. Flat networks give ransomware nowhere to stop, and most clinical devices can't run endpoint protection, making network-level controls the last line of defense. The shift from basic virtual local area networks to identity- and policy-based access through network access control and zero trust frameworks means the right controls follow users and devices wherever they connect, not just inside the building.

Learning objectives:

- Apply identity- and policy-based access controls to design segmentation strategies that secure users and devices across on-site and remote healthcare environments
- Compare traditional virtual local area networks-based segmentation with modern approaches, including network access control and zero trust frameworks, to understand differences in security effectiveness
- Explain the role of network segmentation in preventing ransomware spread and protecting clinical environments where endpoint security is limited or unavailable

12:15 p.m. **Lunch and networking**

1:15 p.m. **From Exposure to Exploitation: How Real-World Threats Target Healthcare Organizations**
Zach Furst, Chief Information Security Officer, University of Iowa/UI Health Care, and Charity Sharpe, Chief Information Security Officer, UnityPoint Health

Healthcare organizations are facing an evolving threat landscape where attacks increasingly target the broader workforce, trusted identities and external exposure points, not just the network itself. From executive impersonation and payroll fraud to account takeovers, lookalike domains and third party breaches, today's threats exploit both human behavior and digital footprints. In this session, healthcare cybersecurity leaders will share real-world examples and practical insights into how these attacks unfold and how organizations detect and mitigate them. Attendees will gain a clearer understanding of emerging threat patterns and strategies to strengthen monitoring, reduce exposure and protect the workforce and organization.

Learning objectives:

- Examine how modern attacks exploit human behavior and digital identities by analyzing real-world examples shared by healthcare cybersecurity leaders
- Identify key healthcare cybersecurity threats, including executive impersonation, payroll fraud, account takeovers and third-party breaches
- Implement strategies to enhance organizational security, including improving monitoring practices, reducing external exposure, and protecting workforce identities and systems

2:15 p.m. **Break and networking**

2:30 p.m. **AI in Healthcare: What's Real, What's Risky and What's Next**
Brice Jager, Information Technology Director, Myrtue Medical Center

AI is moving quickly into healthcare, but the conversation is often split between hype and fear. This session will provide a practical look at what AI is, how it's being used, where the risks live and how healthcare organizations can approach AI responsibly. The question is not just whether healthcare can adopt AI, but whether it can do so safely and securely.

Learning objectives:

- Apply principles for responsible AI implementation to ensure safe, secure and trustworthy use
- Assess the risks and challenges associated with the adoption of AI, including privacy, security, bias and trust
- Define AI's core healthcare concepts, including common applications, capabilities and limitations

3:30 p.m. **Closing**
Gary Davis, Vice President, Information Technology Operations and Security, Iowa Hospital Association, Des Moines

PROGRAM INFORMATION

IHA Conference Center, 100 E. Grand Ave., Ste. 100, Des Moines.

- If you have dietary restrictions or allergies, email iharegistration@ihaonline.org.
- The dress for the conference is business casual. IHA recommends layered clothing for your comfort.
- This is a paperless conference. IHA will email conference materials when available.

ADA POLICY

IHA does not discriminate in its educational programs based on race, religion, color, sex or disability. IHA wishes not to exclude, deny services, segregate or treat anyone with a disability differently because of the absence of auxiliary aids and services. If you need auxiliary aids or services under the Americans With Disabilities Act to attend this conference, contact the IHA Education Department at 515-288-1955 or iharegistration@ihaonline.org.