PYA 2025 Summer CPE Symposium, Session 4 – After the Breach: Navigating the Fallout of Healthcare Data Compromises

Presented June 19, 2025 by PYA's Barry Mathis | Part of the PYA 2025 Summer CPE Symposium Webinar Series

https://www.pyapc.com/insights/summer-symposium-session-4-after-the-breach-navigating-the-fallout-of-healthcare-data-compromises/

Please note, this transcript was generated automatically. PYA cannot guarantee its accuracy or completeness.

WEBINAR SUMMARY

In this webinar, PYA Principal Barry Mathis explores what healthcare organizations should do *after* a data breach has occurred, focusing on the critical phases of containment, eradication, and recovery. Using real-world examples and firsthand consulting experience, Barry outlines practical steps and lessons learned from organizations affected by ransomware, vendor breaches, and failed backups. The presentation emphasizes cross-functional collaboration, legal involvement, and the need to regularly test not just backup systems, but recovery capabilities. Barry also underscores the importance of preparing tabletop exercises based on actual healthcare breach case studies—rather than hypothetical scenarios—to truly test organizational resilience.

Key topics include:

- Activating and optimizing your incident response plan
- Implementing a zero-trust environment to limit horizontal movement
- The role of cyber insurance and approved partners in breach response
- Importance of preserving forensic evidence for regulatory and legal review
- Best practices for internal and external communication
- Real-world case study: six-month PACS recovery timeline due to outdated systems

WEBINAR HIGHLIGHTS AND FREQUENTLY ASKED QUESTIONS

What should a healthcare organization do first after a data breach?

- Immediately activate your incident response plan. This includes isolating affected systems, notifying key stakeholders (including legal counsel), and preserving forensic evidence.

What is a Zero-Trust Environment and why is it important after a breach?

- A zero-trust environment assumes no implicit trust within a network. It continuously verifies identities and activities, limiting attackers' lateral movement. It's essential for both breach prevention and containment.

How does cyber insurance impact breach response?

- Cyber insurance policies often dictate the use of specific vendor partners for breach investigation and remediation. Failing to follow reporting requirements may void coverage or reduce reimbursement.

Why is it critical to preserve forensic evidence after a breach?

- Forensic evidence is essential for understanding what happened, determining regulatory obligations, and defending against civil litigation. Proper preservation should be guided by legal counsel.

What are common missteps in breach notification?

- Prematurely notifying stakeholders or the public without confirming a breach can trigger regulatory scrutiny and reputational damage. Coordination with legal and PR professionals is key.

How long does it take to recover systems after a breach?

- Recovery time varies. In one case shared during the webinar, restoring a compromised PACS took six months due to outdated systems and poor vendor support. Recovery planning must include all critical systems—not just EHR and email.

How often should healthcare organizations test recovery processes?

- Regularly. Tabletop exercises and full recovery drills are essential. Focus not just on data backups, but on whether systems can actually be restored and function properly.

What role do attorneys play in breach response?

- Legal counsel ensures compliance with HIPAA, state laws, and breach notification requirements. They also help maintain attorney-client privilege, which is important if litigation arises.

Are healthcare breaches usually caused by internal failures or external threats?

- Most recent breaches stem from external threats, especially third-party vendors. However, internal gaps—such as weak MFA or legacy systems—amplify risk.

How can organizations prepare more effectively for a breach?

- Develop and regularly update an incident response plan, test your backups and restoration processes, engage external cybersecurity support in advance, and use actual breach case studies in tabletop exercises.

ACTION ITEMS

- Review the organization's incident response plan and communication protocols. Involve legal counsel.
- Ask IT team about the organization's use of zero-trust security principles.
- Assess the organization's ability to recover critical systems like PACS in the event of a breach. Test backup and recovery procedures.
- Conduct tabletop exercises based on real-world breach scenarios, not hypothetical ones.
- To contact PYA to learn more and schedule a breach readiness assessment and/or tabletop exercise, please visit PYA's cybersecurity services page at https://www.pyapc.com/services/cybersecurity-risk-solutions

WEBINAR OUTLINE

Introduction and Overview of the Webinar

- Barry Mathis discusses his background in software, data systems security, and healthcare compliance through his extensive experience in IT and CIO roles.
- Barry shares his personal experience with cyberattacks and the importance of learning from them.
- He outlines the goals of the presentation, focusing on what happens after a breach and the importance of preparedness.

Immediate Actions After a Breach

- Barry Mathis discusses the importance of having an incident response plan in place.
- He shares examples of immediate actions taken during breaches, including sending out notices prematurely and disconnecting data centers.
- Barry introduces the concept of zero-trust environments and their importance in preventing lateral movement of bad actors within an organization.
- He mentions the Change Healthcare breach as a significant example of the need for zero-trust.

Eradication and Recovery Phases

- Barry Mathis explains the eradication phase, which involves removing malware and ensuring no traces remain.
- He highlights the importance of cyber insurance companies in the eradication process and the need for multiple layers of validation.
- Barry discusses the recovery phase, emphasizing the need for thorough sanitization and the potential financial impact of breaches.
- He shares a case study of a hospital CEO who experienced a breach, and the challenges faced in restoring systems.

Communication and Legal Considerations

- Barry Mathis stresses the importance of clear communication during an incident, including notifying internal stakeholders and engaging cybersecurity experts.
- He advises preserving forensic evidence and involving legal counsel early to ensure compliance with breach notification requirements.
- Barry discusses the regulatory implications of breaches, including state-specific requirements and the need for thorough investigations.
- He shares tips for conducting effective tabletop exercises and using real-world scenarios to test preparedness.

Long-Term Impact and Prevention

- Barry Mathis discusses the long-term impact of breaches, including financial costs, reputational damage, and the need for ongoing recovery efforts.
- He emphasizes the importance of investing in effective cybersecurity training and regular audits.
- Barry highlights the role of multi-factor authentication and zero-trust environments in preventing breaches.
- He shares a case study of MD Anderson's fine reduction due to their proactive measures and the importance of demonstrating compliance.

Final Thoughts and Recommendations

- Barry Mathis advises having a chief information security officer or a dedicated information security team.
- He emphasizes the critical need for multi-factor authentication and regular audits to maintain security.
- Barry details the importance of transparent communication and the role of public relations firms in rebuilding trust after a breach.