HTAA IT Institute
Health IT Training By Healthcare Professionals

Change Healthcare Cyber Breach

Lessons Learned and What Every Health Center Should Do

Change Healthcare (Change), a subsidiary of United Health, is one of the largest healthcare technology companies in the U.S. Change provides payment and revenue cycle management, clinical decision support, imaging and patient engagement services to a wide range of healthcare provider organizations. On Thursday February 21, Change realized they were hit with a cyber attack that disrupted key systems and operations. Due to security, reputational and financial reasons, Change has been tight-lipped about what caused the cyber breach. They did tell their customers to disengage and disconnect from Change systems. One big effect is that Change users have been unable to process insurance eligibility and claims for over 5 days.

While it is impossible to totally prevent a potential data breach, it is very possible to be prepared and reduce the downtime and costly operational disruption to your organization. Every healthcare organization should make sure they do the following activities on a regular basis.

- Validate third party vendor compliance with all HIPAA HITECH requirements
- Ensure all known critical vulnerabilities have been patched. Run a vulnerability scan to identify potential hardware and application vulnerabilities and develop mitigation plans
- Test the redundancy and resiliency of all network infrastructure components and the validity and ability to utilize data backups
- Review and test the organization's cyber incident response and IT continuity plans to ensure they are up to date and integrate with the overall organization emergency operations plans
- Ensure network monitoring tools are operational and monitoring output is reviewed on a periodic basis for any unknown activity
- Continuously remind the entire health center organization on good security practices through regular cybersecurity risk awareness updates
- Ensure health center leadership understands the risk to the organization from a cyber security attack and the resources needed to best manage the risk

Healthcare continues to be the most attacked and breached industry, implementing proactive cyber and data security practices can reduce the risk.

Contact us:
info@htaaitinstitute.org
301.941.3366
htaaitinstitute.org

Powered by: HEALTH TECH ACCESS ALLIANCE