asureti

Privacy Gap Risk Analysis
Case Study

Regional Healthcare System

Kansas, United States

Founded in 1998, this healthcare system is a world-class academic medical center and destination for complex care and diagnosis.

Key figures:

- Physicians that represent more than 200 specialties.
- Over 900 staffed beds.
- 47,771 annual emergency department visits.

asureti

The Challenge

This healthcare system came to Asureti concerned about potential gaps in their data collection and data privacy processes. They wanted an independent analysis and complete picture of privacy risks within their web portals and patient-facing applications. Without this knowledge, they could be vulnerable to unexpected fines or litigation. **Worse, they could be putting patients at risk!**

Associated Business Risks

Loss of PHI

Loss or unknown sharing of Protected Health Information (PHI) data associated with a patient of the hospital puts individuals at risk.

Potential Litigation

Violations of the HIPAA Privacy Rule could equate to exhaustive litigation, huge fines and required compliance monitoring.

Impacted Reputation

Breach of patient trust can have devastating consequences on the healthcare system's good standing.

asureti

Our Approach

We took an approach similar to a forensic investigation within the hospital's technology systems and associated processes:

1. Identified all tools and technology involving patient information. This inventory provided technical insight and a foundation for the next steps.

2. Interviewed key employees throughout the healthcare network with potential access to PHI to fully understand their internal processes. We worked as an extension to the internal team to analyze current processes and identify potential concerns.

3. Completed a technical analysis on protected data storage and movement throughout the network to identify potential HIPAA violations.

4. Established a steady cadence of reporting that was shared with healthcare system leadership, streamlining information regarding exposures and recommended actions.

asureti

Our Analysis

After interviewing employees, and identifying all tools and technologies involving the healthcare system's **25 websites,** we found:

- Extensive use of third-party tracking tools needing further configuration for protection of PHI.
- Lack of comprehensive documentation regarding how data was being collected by the websites.

Our technical analysis included a firewall log analysis *and* installed software analysis to determine what information was being collected. We analyzed:

- Online tools (pdf uploading, Google apps)
- Screen sharing/Screen recording tools
- Third-party tracking tools
- Contracted tools (partnered company's tools)
- Social media tools
- Ad networks (Doubleclick, Adserv, Amazon, etc.)

We concluded that the healthcare system was vulnerable to unexpected PHI data loss and required certain actions to confirm full alignment with PHI regulations.

asureti

Recommended Actions

Immediate:

- Train hospital staff on proper data protection policies. Empower designated teams to be data privacy experts per the organization's policies.
- **Stop** using third-party tracking tools where they do not own the data collected.
- Confirm vendor business associate agreements (BAAs) are appropriate to protect PHI data.
- Identify and approve business-necessary screen recording/screen sharing software.
- Restrict usage of personal social media accounts and other online tools within the company networks.

Long Term:

- Engage a trusted partner to evaluate PHI protection effectiveness at least once a year.
- Yearly internal PHI policy evaluation to confirm updates and program enhancements are followed.

asureti

Project Recap

6,000
Pieces of Software Evaluated

3,000
Firewall Log Entries

25
Websites Evaluated

By partnering with a knowledgeable and trusted GRC team, the healthcare system has the necessary information to enhance internal processes and systems to avoid potential fines and litigation. The outcomes of this project also provided increased abilities to manage data sharing and ownership data more effectively.

This partnership involved monitoring the entire online presence of the healthcare system, confirming proper PHI and security procedures were created.

By discovering privacy roadblocks, we provided a route to mature their data privacy program and promote enhanced patient experiences.

asureti

Similar Challenge?

Book a discovery call

Email

info@asureti.com

asureti