It Pays to Be Cyber Secure

Robert Zimmerman, rzimmerman@healthtechalley.com

Healthcare continues to be the number one attacked industry. COVID-19 has increased data and cybersecurity risk as more threat agents target healthcare data. Yet many smaller healthcare organizations and business associates continue to believe a breach can't happen to them and under invest in security. It doesn't have to be costly and overwhelming to be cyber secure.

Today technology is more complex and ever present in healthcare. Data in electronic format is ever more prevalent and susceptible to loss and or a data breach. COVID-19 has made healthcare data extremely valuable. Data security threats are increasing every day. Just check the news on any given day. Ransomware and malware attacks were up 400% in 2020. This number doesn't begin to include the thousands of security incidents that are never reported.

But you may ask, "Should I worry if I'm not secure and compliant? Could my business operations be disrupted by a data breach? Should I make the effort to perform a security risk assessment and implement required security processes and controls? Am I prepared if, my customers and partners require me to be HIPAA compliant?". The answers to all of these should be a resounding: *YES!*

Most smaller healthcare providers and business associates continue to deemphasize security. The majority are not cyber secure or HIPAA HITECH compliant. Yet statistics say something completely different. In 2020, almost 80% of healthcare organizations suffered a data breach of some type. At the same time, the size and the cost of a data breach continues to rise.

Small and medium sized healthcare organizations are becoming prime targets of hackers and opportunists. The risks are real, and they need to be managed. Here are just a few:

- Most small and medium businesses underspend on security
- Healthcare records contain large amounts of personal information
- Mass digitization of patient data has greatly increased attack opportunities
- The value to thieves of a healthcare data record is 400 times that of a credit card record
- Mobile devices have become the primary computing vehicle increasing the potential for loss and theft

Most small to medium healthcare organizations have similar security gaps. Do these security gaps sound like the reality in your organization?

- Incomplete or out-of-date risk assessment
- Missing security and privacy policies and procedures
- Limited and check-the-box security awareness training
- Untested disaster recovery and business continuity plans
- Insufficient IT staffing, resources, and management commitment to IT
- Inconsistent network monitoring
- Lack of vendor oversight

It Pays to Be Cyber Secure

Robert Zimmerman, rzimmerman@healthtechalley.com

Remediating security gaps and implementing basic security controls can pay dividends to your organization. It can help you generate more revenue and increase new potential business opportunities. More and more business partners are asking: "Are you secure and HIPAA compliant?". Many will not work with you if you can't answer affirmatively to that simple but important question. Being secure can also be a business development differentiator by reducing the impact of a costly lawsuit over PHI mishandling or access, preventing reputational damage and consumer mistrust, and minimizing potential fines from breaches and audits. It doesn't make sense for you to believe a data breach won't happen to you and gamble the well-being of your organization.

So, what steps should you take right now? At a minimum, you should complete basic data security activities to minimize risks and be prepared to respond to business partners and new customer requests. This means completing at least the following:

- **Perform a Security Risk Assessment** to understand where PHI is stored and used, identify critical technology risks that must be controlled, and understand what mitigating actions need to be taken.
- **Conduct a Gap Analysis** to prioritize remediation activities and develop a work plan to systematically close identified security gaps.
- **Develop a Workplan** to have a plan and strategy so progress can be measured and tracked.
- **Remediate Critical Risks and Implement Mitigating Controls** to reduce risk and implement a secure and protected environment. Key activities include:
    - Develop/Update and implement security and privacy policies and procedures.
    - Implement ongoing monitoring tools to ensure policies are followed and to secure your technology, networks and physical environments
    - Develop/Update Key Risk Management Plans including
        - Incident Response
        - Disaster Recovery
        - Contingency/Business Continuity
        - Physical Security
- **Perform ongoing vulnerability assessments** of networks and devices to ensure software and physical vulnerabilities are quickly identified and remediated.
- **Conduct workforce training** to ensure staff understand what security risks exist and what actions every staff member must do daily to maintain a secure environment.

Your organization and you can be cyber and data secure. It just takes focus. Make the effort!

The time for taking steps to secure your organization and protected health information is now. Security needs to be a priority. Becoming secure and compliant doesn't have to be cost prohibitive or overwhelming. The investment in cybersecurity safeguards will pay for itself many times over. Get ahead of the curve. ***Bottom line…It pays to be Cyber Secure!***