SKYVIEW TECHNOLOGY

HIPAA & THE DARK WEB

January 2020

www.SkyViewTechnology.com

EXPOSED PATIENT DATA IS QUICKLY BECOMING A SOUGHT-AFTER COMMODITY ON UNDERGROUND MARKETPLACES SUCH AS THE DARK WEB.

Maintaining compliance in today's ever-changing environment is no easy task, particularly within the healthcare space. In the past, hackers opportunistically targeted providers due to poor security networks and infrastructure. Over time, however, cybercriminals have realized the true value of personally identifiable information (PII) and protected health information (PHI), which can be leveraged for identity theft, financial fraud, and other lucrative attack types. Exposed patient data is quickly becoming a sought-after commodity on underground marketplaces such as the Dark Web, forcing companies and MSPs to take notice.

Follow along as we provide a snapshot of the Health Insurance Portability and Accountability Act (HIPAA) today and discuss its implications for your business.

SKYVIEW TECHNOLOGY

www.SkyViewTechnology.com

HISTORY OF HIPAA

Established in 1996, the Health Insurance Portability and Accountability Act was introduced by the Department of Health and Human Services (HHS) to set standards for data security and privacy in the healthcare sector. The legislation was passed with good intentions but designed for a world that still operated using paper records. As technology drastically shifted market dynamics, some of the provisions quickly grew outdated.

Nevertheless, the Security Rule has passed the test of time in many ways, providing administrative, physical, and technical safeguards for protecting individuals' electronic personal health information.

CYBERSECURITY GUIDELINES

In December of 2018, HHS issued new cybersecurity guidelines in an effort to drive voluntary adoption of best practices. Such guidance could signal impending legislation to come in the near future, so our experts curated some key takeaway.

Risk Analysis

Organizations must assess all potential risks and vulnerabilities affecting the confidentiality, integrity, and availability of PHI across their ecosystem. This is easier said than done. Many companies underestimate how far PHI travels inside or outside their networks, which have led to costly HIPAA violations in the past. Determining the need for business associate agreements is a key element of a risk analysis, since they govern how entities handle PHI.

SKYVIEW TECHNOLOGY

2) Social Engineering

As evidenced by recent events, healthcare organizations are often subject to phishing and ransomware attacks. Even though employee training and simulated phishing attacks have been recognized as the best defense to mitigating social engineering hacks, they are rarely facilitated (see graph below). Thankfully, we are able to offer a robust security awareness training campaigns to educate employees and demonstrate the cybersecurity posture of your organization.

Employee Training -
2019 Security Metrics Guide to HIPAA

Semi-Annually	Yearly	Never train	Don't know how often they train
8%	60%	10%	12%

3) Insider Threats

Whether it's born out of innocent curiosity or malicious intention, employee snooping is a serious vulnerability to PHI. Even worse, it can not only result in HIPAA violations, but also be identified as criminal activity by state attorney generals.

As public vigilance of security and privacy continues to increase, being featured in headlines as the victim of an insider attack poses serious consequences for brand equity and customer loyalty.

4) Enterprise Risk Management

Iliana L. Peters, Former Acting Deputy Director for HIPAA at HHS, recommends that organizations partner with solution providers that can perform comprehensive risk management and offer expert counsel. Given that the majority of Office for Civil Rights settlements are related to risk management, organizations have a financial incentive to enlist in IT security best practices and training.

SOLUTIONS

Although ongoing HIPAA compliance may seem like an arduous undertaking, it can greatly benefit your organization from a strategic perspective. Far too often, it's the simple, easy-to-patch vulnerabilities that slip through the cracks and lead to expensive violations or breaches. Even those with advanced defenses can be inadvertently compromised by bad passwords or employee phishing.

However, we're not here to spell out doom-and-gloom. Find out how our experts and solutions can help you:

- Proactively monitor the Dark Web for compromised employee or patient data
- Transform your employees into the best defense against cybercrime with simulated phishing attacks and security training
- Consider implementing Compliance Process Automation

See the next page for our guide below to see how HIPAA compliance varies by state and region.

Far too often, it's the simple, easy-to-patch vulnerabilities that slip through the cracks and lead to expensive violations or breaches.

HIPAA Compliance
by State and Region

State	Reasonable & Appropriate Safeguards	Business Assessment Requirements	Administrative, Physical, and Technical	Penalties	Third-Party Responsibility
Arkansas	X				
California	X	X		X	
Connecticut	X			X	
Illinois	X				X
Indiana	X			X	
Maryland	X			X	X
Massachusetts	X		X		
Nevada	X				X
Oregon	X		X		
Rhode Island	X	X		X	
South Carolina	X		X	X	X
Texas	X				
Utah	X			X	
Washington	X			X	

SOURCES

https://healthitsecurity.com/news/hackers-targeting-healthcare-with-financially-motivated-cyberattacks
https://info.securitymetrics.com/hipaa-guide-2019
https://www.hipaasecurenow.com/index.php/why-we-need-to-go-beyond-hipaa/
https://lockpath.com/contributors/ogden-mike/intersection-hipaa-compliance-data-security/
https://www.hhs.gov/hipaa/for-professionals/security/index.html

SKYVIEW TECHNOLOGY

SkyView Technology offers nearly 2 decades of proactive, award winning, support with an average customer retention of over 10 years. We employ only reliable and certified engineers and offer 24/7 support with a quick response time. Whether you are looking for complete outsourcing or supplemental IT support for your in-house staff, SkyView Technology is there to take the worry out of your IT!

Offices: Charleston-843-872-0945, Charlotte-704-228-0497, Chicago-773-561-4502

- **24/7 Support**
- **Cyber-Security Specialist**
- **Cloud Services**
- **Fully Managed Options**
- **Compliance Specialist**
- **Backup Options**
- **Disaster Recovery**
- **Hardware Installation**
- **Dark Web Monitoring**
- **Supplemental Support**

"It is a pleasure and a relief knowing that I can rely on Skyview 100%. Availability and dedication put forth for clients is immeasurable! Always a consistent level of performance from highly qualified technicians, an absolute understanding of our unique network and the ability to find ways to solve all requests quickly."
Marion, Medical Practice

877-818-3247
WWW.SKYVIEWTECHNOLOGY.COM