Strengthening HIPAA and Cybersecurity Through Staff Education and Phishing Awareness

By Rana McSpadden, FACMPE

In our March Sentinel Article, Expanding Your Cyber Protection, we discussed the transition of our cyber liability carrier from Tokio Marine to Beazley Cyber Insurance and the expanded resources now available to policyholders. This article focuses on the training, education, and phish testing tools available to help practices strengthen their cybersecurity and compliance efforts.

SVMIC provides HIPAA and cybersecurity staff education through our Compliance Center. These recorded webinars are valuable resources for onboarding new employees and

conducting annual HIPAA and cybersecurity training. In addition to annual training, practices may also need to provide supplemental HIPAA education throughout the year. This is especially valuable following a privacy or security incident or when staff fail an internal phishing test, helping reinforce best practices and reduce future risk.

Beazley's Breach Solutions Portal offers 11 training modules that can be assigned to staff, including basic HIPAA, Password Security, Phishing, AI Safety, Working Remotely, among other titles. These modules run between 5 to 40 minutes, with most running 20 minutes. Each session also includes a quiz to test employees' knowledge of the subject, reinforcing learning and equipping staff with the knowledge needed to recognize and respond to potential privacy or security threats.

In addition to structured training modules, practices can further reinforce cybersecurity awareness through simulated phishing testing offered through Beazley's Breach Solutions Portal. This approach provides real-world examples of phishing emails. Phishing attacks continue to be one of the most common causes of cyber incidents in healthcare, making it essential for staff to recognize and respond appropriately. These simulated tests provide a safe environment for employees to practice identifying suspicious emails without the risk of an actual breach while reinforcing awareness through real-world scenarios. Practices can also use the results to identify trends, measure staff awareness, and target additional education where needed. Ultimately, regular phishing testing helps strengthen a practice's overall security posture and reduce the risk of future incidents.

By consistently utilizing the training and phish testing resources available through SVMIC and Beazley, practices can take a proactive approach to strengthening compliance and cybersecurity efforts. Ongoing education not only keeps staff informed but also plays a critical role in reducing risk and supporting a culture of accountability and awareness throughout the organization.

To access these resources through Beazley, visit the Cybersecurity Resource Access page through the SVMIC Vantage account portal. This page provides an access link and step-by-step instructions for creating an Admin account. The link will direct users to the Breach Solutions portal, where the account setup process is completed. Once an Admin account is active, follow instructions on how to add staff email addresses and assign tasks.

If you have questions about HIPAA, cybersecurity, or access to SVMIC resources, call 800-342-2239 or email Contact@svmic.com.

If you experience a cybersecurity or other HIPAA related incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak with the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account here.

The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.