

Supplementing Policies with Beazley Resources



By Rana McSpadden, FACMPE

As discussed in our two previous cybersecurity articles, [Expanding Your Cyber Protection](#) and [Strengthening HIPAA and Cybersecurity Through Staff Education and Phishing Awareness](#), SVMIC is transitioning our cybersecurity insurance provider from Tokio Marine to Beazley Cyber Insurance. This transition gives policyholders access to new cybersecurity resources designed to support their current cybersecurity program.

As practices review these new resources, it may be helpful to understand how they fit alongside SVMIC's existing HIPAA compliance tools. SVMIC currently provides a fully customizable HIPAA Compliance Manual with multiple resources and fillable forms, complimentary to our policyholders through the Compliance Center. While this manual remains a comprehensive resource, Beazley's Breach Solutions offers 30 customizable policies that may serve as a helpful supplement. Practices may use these policies to compare language, strengthen existing procedures, or address specific cybersecurity-related concerns.

Beazley's Breach Solutions policies can serve as a valuable resource for practices seeking to improve their management of system access, vendor relationships, incident response, acceptable device use, password expectations, and other security-related processes. Additional policies addressing training, corrective action, and business continuity are also available.

As with any policy template, these documents should be customized before implementation. Practices should review the language carefully, remove provisions that do not apply, and revise procedures so they reflect the practice's actual workflow, technology, staffing structure, and vendor arrangements. Because these topics often involve both administrative and technical safeguards, practices should include leadership, the privacy or security officer, and the IT department or vendor to participate in the review. Consider having corporate counsel review the policies before final implementation and staff training.

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.