Prevalent
MITRATECH

Neighborhood Health Plan of Rhode Island Immunizes Against Technology Risk with Prevalent

Case Study:
Neighborhood Health Plan of Rhode Island

Founded in 1993, Neighborhood Health Plan of Rhode Island (Neighborhood) is a not-for-profit 501c3 health maintenance organization (HMO) that serves one in five Rhode Islanders. Neighborhood serves over 230,000 members in the state with 84 percent of its membership Medicaid eligible through its ACCESS and TRUST plans and 6 percent of its membership utilizing Neighborhood's INTEGRITY Medicare-Medicaid Plan (MMP).

The Challenge

As a health insurance provider, Neighborhood needs to comply with specific data privacy and data security standards related to the Health Insurance Portability and Accountability Act (HIPAA). Neighborhood's vendor relationships can be a key defense in the company's ability to secure the protected health information of its members from breaches and other cyberattacks. Part of this protection strategy, according to Senior Information Security and Risk Analyst John Turschman, lies in assessing vendors for specific risks related to data security and privacy. John's department is responsible for these vendor risk assessments, which are done as part of the vendor onboarding process.

"Once we identify that a new or existing vendor needs deeper risk insight, we send them a SIG Lite assessment to fill out. That survey then helps us determine what sort of security or data risk the vendor presents and define next-step mitigations," John said.

Neighborhood has specific challenges around vendor response, process management, and tracking potential vendor risks outside of assessments. Ensuring HIPAA compliance requires vendors to understand the risks they've accepted and put in place specific internal mitigations to reduce the risk of electronic protected health information (ePHI) data loss. As a result, Neighborhood needs a solution to help them assess the data security risk in their technology supply chain and determine appropriate mitigations to comply with healthcare regulations.

Neighborhood Health Plan OF RHODE ISLAND™

Industry: Health Insurance

Location: United States

Solution: The Prevalent™ TPRM Platform, Vendor Risk Assessment Managed Services, Vendor Threat Monitoring

Benefits:

- Central, easy-to-update risk register for data privacy and security issues
- Increased visibility into vendor risks throughout the technology supply chain
- Improved security posture and HIPAA compliance insight through risk assessments and remediation

"Prevalent risk assessment capabilities have been a key part of helping us ensure the security of our member data. As a health insurer, we have specific responsibilities to our members and the Prevalent Platform has helped us ensure that our vendors have the capabilities they need to protect our sensitive data and reduce our technology risk."

- John Turschman
Senior Information Security and Risk Analyst
Neighborhood Health Plan of Rhode Island

The Solution

Neighborhood Health Plan of Rhode Island uses the Prevalent™ Third-Party Risk Management Platform (TPRM) for vendor risk assessments, managed services for risk remediation, and continuous risk monitoring for regular insights. Once a new vendor is added or if there is an existing vendor identified that has never done a risk assessment, Neighborhood sends them a SIG Lite survey via Prevalent for the vendor to fill out.

The Prevalent Platform empowers Neighborhood to identify risks via the assessment and determine next steps to remediate any issues. Neighborhood uses Prevalent as a key part of building a cohesive third-party risk management program at the company and are currently working to scale that component of their operations.

"Prevalent risk assessment capabilities have been a key part of helping us ensure the security of our member data. As a health insurer, we have specific responsibilities to our members and the Prevalent Platform has helped us ensure that our vendors have the capabilities they need to protect our sensitive data and reduce our technology risk," John said.

Neighborhood also uses Prevalent managed services to assist with risk remediation and contextual reporting. This streamlines the ability to determine appropriate mitigation actions and residual risk within their vendor universe. It also empowers the growth of the Neighborhood third-party risk management program beyond assessments to provide additional enterprise risk context for senior leaders.

Results

Before implementing Prevalent, Neighborhood did not have a third-party risk management program. Now that they've fully deployed the Prevalent platform and worked through developing their TPRM program with the help of Prevalent staff, they have a comprehensive view into their vendor risks and can mitigate potential issues with the security of member health information.

"As a health care organization, we're going to do business with hospitals and other entities in the healthcare sector. Understanding the risk of doing business with these organizations is very important for our security. Performing the risk assessments with Prevalent means that we're able to identify if a vendor doesn't have the right encryption or the right password policies, for example," John said.

Prevalent has empowered Neighborhood with a more robust security posture because of the visibility the solution has created to more accurately identify technology supply chain risks and communicate those out to the business has created the sense of better protection internally. Even if vendors choose not to remediate the identified issues, identifying security risks makes it possible for Neighborhood to include mitigations on their end.

John said he's looking forward to continuing to work with Prevalent as the TPRM program at Neighborhood continues to evolve and mature over time.