Healthcare Industry Case Study: Preventing Data Breaches with Safer, Smarter Identities

How Horizon BCBSNJ found a more secure, usable and affordable alternative to traditional healthcare identification cards.

The Challenge

The healthcare industry is experiencing an epidemic. According to the 2018 Verizon Data Breach Investigations Report (DBIR), the past year alone saw 536 healthcare breaches. The healthcare system is a prime target for cybercriminals due to its highly valuable data – one stolen healthcare record is worth more than 10 times the value of a Social Security number on the cyber black market.

Such valuable confidential data requires a level of secure identity verification practices that are not currently being implemented. Passwords are the most widely-used form of verification today, but they are also the least secure. 81 percent of breaches leveraged stolen and/or weak passwords, as indicated in the 2017 DBIR. They can also be frustrating to use as many companies employ requirements for frequent resets with complicated, hard-to-remember passwords.

Healthcare organizations looking to implement stronger authentication methods than passwords need a solution that can provide convenience, accessibility, security and compliance with regulatory standards. To fulfill this need, Horizon Blue Cross Blue Shield of New Jersey (HBCBSNJ) implemented a smart card-based identity system for 7,000 employees across 6,400 laptops in only six months.

The First Steps

HBCBSNJ partnered with Axiad IDS to develop a strategy for securing identity data. With extensive research on technical and procedural techniques and efforts to secure key stakeholder buy-ins, HBCBSNJ prepared to deploy a new trusted identity solution. When weighing options, HBCBSNJ examined factors including cost, scalability and alignment with industry standards, as well as the ability to improve security with more convenience and reliability than password-based authentication. This was followed by a rigorous evaluation and proof-of-concept phase to ensure feasibility.

HBCBSNJ chose a multi-factor smart card and PIN ID badge solution for employee access to facilities and login access to data records. The solution provided the opportunity to integrate with pre-existing hardware and helped to avoid added costs from bringing in third-party resources. The solution is also one of the only two methods that meets NIST 800-63-2 highest security requirements, providing both HBCBSNJ and stakeholders with a high degree of confidence in the new implementation.

The Rollout of a Strong Multi-Factor Authentication Solution

In phase one, HBCBSNJ implemented a smart card-based identity badge system for 7,000 employees across 6,400 laptops in only six months. The deployment started with local laptops, followed by virtual private network (VPN), internal web applications, digital signature and email applications. Strong monitoring and enforcement policies have created a feedback loop that ensures employees are able to quickly and seamlessly adopt new smart card login practices.

One of the goals of this new approach is to build a trusted community – inclusive of employees and facilities and the patients they care for. Phase two is underway to bring a smart card- and/or mobile-based identity system to patients.

The Results/Impact

HBCBSNJ successfully rolled out the smart card solution to 6,400 laptops/desktops in an accelerated deployment of just six months, made possible by the preparations they made regarding research and buy-ins from stakeholders.

Outcomes achieved from this phase of the project included cost reduction, decline in the need for help desk intervention, improved data security, and secure and easy access to medical records. HBCBSNJ was able to quickly deploy a strong and proven smart card solution — with little additional technology or investments — by leveraging standards resulting from a decade of investments made in high-security smart card identity badges and security solutions used by the federal government. Operating with full knowledge and securing buy-in from key HBCBSNJ stakeholders up front helped them avoid both administrative hiccups and technical issues frequently faced when transitioning a large organization to a new trusted identity security system.

The new smart card badging solution significantly lowered the risk of data breaches while creating a simplified user experience. Login via a smart card combined with an eight-digit numeric PIN is easy to use and eliminates the frustration of frequent password changes. Company town halls reported very high satisfaction with the new system among employees.

With the smart card badging solution, HBCBSNJ addressed the desire to instantly provide a high degree of confidence when it came to data security. This solution lowered up-front investment, leveraged the existing physical access control system, enabled rapid login time and provided platform flexibility. Based on the success of this solution, HBCBSNJ will begin phase two of their rollout: bringing patients into the secure ecosystem.

About the Secure Technology Alliance

The Secure Technology Alliance is the digital security industry's premier association. The Alliance brings together leading providers and adopters of end-to-end security solutions designed to protect privacy and digital assets in payments, mobile, identity and access, healthcare, transportation and the emerging Internet of Things (IoT) markets.

The Alliance's mission is to stimulate understanding, adoption and widespread application of connected digital solutions based on secure chip and other technologies and systems needed to protect data, enable secure authentication and facilitate commerce.

The Alliance is driven by its U.S.-focused member companies. They collaborate by sharing expertise and industry best practices through industry and technology councils, focused events, educational resources, industry outreach, advocacy, training and certification programs. Through participation in the breadth of Alliance activities, members strengthen personal and organizational networks and take away the insights to build the business strategies needed to commercialize secure products and services in this dynamic environment.