



Bay Medical

A 5-Year Case Study

2FA
Strong Authentication. Simplified.



Bay Medical: A 5-year review on smart card deployment

The Customer

Bay Medical, a 323-bed regional medical center located in Panama City, provides hospital care and outpatient services to patients from a seven-county region in Northwest Florida. It is renowned for clinical excellence, including a Top 50 Hospital Award for three years in a row. Bay Medical has more than 250 physicians on staff representing virtually every medical specialty, and a support staff of more than 2,000 dedicated employees. In 2007, Bay Medical chose 2FA's technology to secure their logon process with smart cards.

Challenges & Objectives

When looking to deploy smart cards, Bay Medical had three main objectives:

1. To ensure HIPAA compliance with strong authentication while accelerating login times and securing audit and logging trails

The first challenge was meeting HIPAA regulations for secure access to patient information, including two-factor authentication, as well as logging all transactions with a patient's medical record. In addition, care providers must have secure access while providing timely patient care. Previously, security had been secondary to fast information access.

When faced with complicated password requirements and lengthy sign-on processes, healthcare providers became frustrated. In an effort to improve provider ease-of-use and patient satisfaction, the IT department created generic accounts for these workstations, relying on the security of individual applications and securing the connection to Citrix desktop and applications. However, this approach left a high risk of security breaches and an inability to log activity of individual users.

2. Freedom to leverage the same cards for physical and logical access

Always seeking to provide the best in physician satisfaction and patient care, Bay Medical needed a solution that could adapt to their changing physical access card needs.

3. Reduce helpdesk calls for password resets.

Ever-changing, complex password requirements were necessary to comply with best security practices, but the normal associated volume of helpdesk calls for password resets became cumbersome and inefficient. In the new solution, Bay Medical searched for a solution to streamline this process, reducing volume (and cost) associated with secure logical access.

“ ...2FA support has been
second to none”



The Environment

The environment at Bay Medical mirrored many large healthcare organizations today, and like others, administrators were continually looking to new technology to improve efficiencies for doctors and patient satisfaction. They were interested in “future-proofing” the solution, such that they could adopt new technologies down the road without re-badging their entire user population, or duplicating major investments in time and resources.



The Solution

The solution, deployed in 2007 and still in use today, included 2FA's strong authentication software and smart cards to support and manage the deployed certificates and smart cards. The single sign-on component sped access to critical applications. IGEL provided a thin client to integrate both hardware and software. Implementing public key infrastructure also added support for digital signatures and non-repudiation for all physicians.

This combination:

- Met HIPAA regulations for positive authentication of providers
- Ensured credibility of audit and logging trails
- Facilitated quick access to workstations and apps
- Enabled software and hardware to be combined into one device - streamlining the equipment and making adherence to security policies straightforward and intuitive.

Security without the hassle

With their smart cards and the software developed by 2FA, Bay Medical's access to applications was made the most secure in the industry, while eliminating the need to keep track of multiple identification cards and passwords.

For example, a doctor uses the same smart card for network access via the IGEL thin client, as well as for physical access into the hospital, including photo personalization and other imprinting to prevent forgery. This increased security comes without the traditional additions for administrative time and expense. Using the credential management portion of 2FA's solution, Bay Medical's IT group can efficiently enroll, issue, renew and revoke credentials. Their administration team chose to utilize a "white glove" approach where they enroll on behalf of their users, which is streamlined within 2FA's web portal. This workflow makes it easy to ensure that when doctors are given their cards, they just change the PIN to one of their choice, and they are ready to log in anywhere in the environment.

When they leave, the provider just needs to remember to take their badge with them, and upon removal from the reader, the user is immediately logged off - securing the workstation with no hassle.

Less spent on maintenance and administration of network access

By going to a two factor authentication model - in this case, card plus PIN - the need to change passwords was virtually eliminated. Physicians found it much easier to remember a PIN than an ever-changing complex password. Also, by combining the logical access with the same badge used for physical building access, doctors lost or "forgot" their credentials at a negligible rate, already being in the habit of bringing their ID to the hospital.

When originally deployed, Bay Medical utilized 2FA to provide the first-ever provisioning of .NET smart cards for enterprise use outside of Microsoft. However, the real versatility of the solution shone when Bay Medical had the flexibility and freedom to purchase HID Crescendo C200 smart cards within the same management system. Physicians did not need to know which card they had; the operation was intuitive and identical. Just as important, administrators did not have to change any processes, allowing seamless transition of mixing the card deployments. This enabled Bay Medical to not only save thousands of dollars, but also to choose the card technology which best matched their own needs, timeline, and cost restraints. Ultimately, the .Net cards were phased out completely and replaced with Crescendo cards across the organization, which are still in use today.



The Final Result

Five years later, David O'Daniel, of ACS, the outsourced IT department for Bay Medical, says "This solution has been a physician-satisfier. There is a huge convenience factor and 2FA support has been second to none."

In addition to increased security measures, the integrated credential management, single sign-on, and thin client solution:

- Provided secure, intuitive, accelerated workstation access for providers
- Eliminated continuously logged on workstations, no longer allowing doctors to "piggy-back" off one session without any useable audit trail
- Utilized the same badge for physical building access and network access
- Digital signatures for non-repudiation and network logon
- Deployed industry-leading technology (several "firsts")
- Sped access to critical applications, while maintaining secure workflows and audit trails