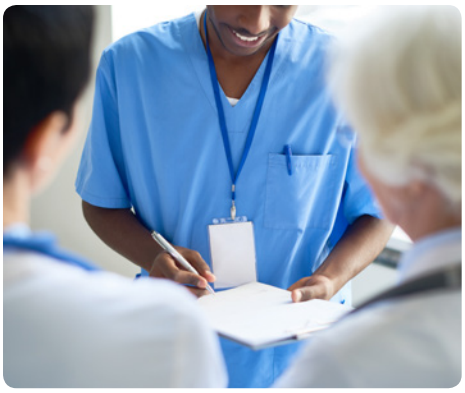
CASE STUDY

Rural Healthcare Provider Invests in Cyber Security



"Once the auditor saw our smart ID badges in action around our environment of care, he ticked off seven of ten compliance elements and made a short day of the successful audit."

Hospital IT Security Administrator

Solutions:

- ActivID® Multi-Factor Authentication Technology
- HID Professional Services

Mid-West, United States

Size doesn't matter to the cyber terrorists who are launching cyber attacks against small hospitals. A rural community healthcare provider with 250+ employees desired to improve how it safeguards patient information. To ensure compliance with Drug Enforcement Administration (DEA) requirements and Health Insurance Portability and Accountability Act (HIPAA) Security Rules, this rural medical center in the Mid-West adopted two-factor authentication for clinicians to secure their credentials, preventing forgeries and reducing risk of data breaches.

The medical center looked no further than the identity technology vendor that provides the physical access control readers on their facility's doors as well as the ID badges in their hands – HID Global, a leader in trusted identity solutions – to create a trusted digital environment at the hospital.

Recognizing the convergence of people's identities across location and digital boundaries, HID has become a one-stop shop for scalable physical access and digital identity solutions – affordable even in the most remote, rural areas.

Challenges

Protecting the access of electronic personal health information (ePHI) was a complex challenge for a hospital with limited resources. HIPAA requires that an individual or an entity accessing ePHI must be authenticated – verified – before access is granted. Like all healthcare providers under HIPAA, the hospital is expected to implement security measures that are sufficient to reduce risk and vulnerabilities, ensuring the confidentiality, integrity and availability of protected health records.

Moreover, the DEA requires that clinicians who are engaging in e-prescribing of controlled substances (EPCS) must adhere to strict requirements, including identity proofing and applying a two-factor authentication protocol with a FIPS 140-2 certified credential. The hospital also recognized that digital prescribing of schedule II-V narcotics is also a valiant way to beat down the opioid crisis.

While the requirement is clear, the problem was that this medical center in a rural part of the Mid-West did not have two-factor authentication capabilities, so its leadership team investigated a Presidential directive that sent them in the direction of HID Global.

Solution

To address the requirements it had to meet, the medical center used the Homeland Security Presidential Directive-12 (HSPD-12) as a template and guideline to create their own program for identity & access management (IAM). HSPD-12 sets policy for a common, reliable and secure identification standard for federal employees and contractors.

When the medical center's team investigated what products the U.S. government was using for logical access, they discovered that many agencies in the federal government use HID ActivID multi-factor authentication technology.

The medical center was already using HID physical access control products (cards and readers), AsureID® software and HID FARGO® printers /encoders for card personalization and issuance. Based on their history of proven success with HID products, the medical center chose to standardize on the HID ActivID platform for multi-factor authentication using FIPS-certified Crescendo ID smart badges.

Because of limited bandwidth, the hospital also relied on HID Professional Services for successful deployment of the feature-rich, future-ready identity management platform.

Benefits

By using HID's identity & access management solution, this rural medical center is able to equip their employees with smart ID cards that can be used for the following:

- Logical access onto the hospital's corporate network and workstations
- Electronic prescriptions of controlled substances (specifically for clinicians)
- Physical access into buildings/rooms and cabinets
- Time-and-attendance
- Single sign-on (SSO) to the hospital's EMR system and all web-based applications
- Email digital signatures and encryption
- Derived credentials
- Certificate-base authentication

These capabilities deliver a variety of benefits that the hospital values, including:

- Higher security
- Compliance with government regulations
- Increased efficiency
- Greater productivity
- Cost savings
- More flexibility
- Ease of use

"Once the auditor saw our smart ID badges in action around our environment of care, he ticked off seven of ten compliance elements and made a short day of the successful audit," stated the hospital IT Security Administrator.

Ultimately, the HID solution for this rural community medical center provides peace of mind by safe-guarding sensitive information and minimizing insider threat risks, while complying with HIPAA, DEA, PCI-DSS and GDPR requirements. With HID's technologies, the identities of people who access online resources, go in and out of the secure areas, and prescribe drugs to patients can be trusted.

2018-03-06-hid-rural-healthcare-cs-en PLT-03740