

Hospital Takes Protection of Sensitive Data from "Risky" to "Responsible"

As the IT director for a regional hospital, I'm mandated by HIPAA to protect our patient's personal medical data and secure our computer networks from unauthorized access.

Industry best practices suggest the best way to achieve these requirements are by:

- Implementing strong logon password policies
- Assigning unique passwords to every account
- Preventing staff members from sharing their passwords, and
- Changing passwords every sixty days.

These cybersecurity measures, while secure, are both burdensome on our busy nurses and doctors; and expensive for IT to manage. Passwords became difficult for the hospital staff to remember and type, which required the IT department to constantly reset forgotten passwords. Resetting passwords wastes time and lowers the hospital's productivity.

Therefore, we need a solution that combines:

- Cybersecurity best practices
- Meets HIPAA MFA compliance regulations
- Makes user logon convenient, and
- Is affordable for the hospital

Security Challenges

Access Smart has always believed that the problem with passwords is with their management, and not their security. That's what Power LogOn fixes.

Power LogOn delivers a secure and convenient way for the medical staff to access their computers without knowing, typing or managing any passwords.

IT no longer has to reset forgotten passwords. And it's an add-on application to your existing employee ID badges.

Here are some of the hospital's Security Challenges.

1. **Add logon security to our existing building access control ID badges.**

The hospital already uses a Mifare card for building access and we need to leverage that investment for cybersecurity access.

2. **Users need to quickly access information from any network terminal.**

Our nurses and doctors are constantly on the move. They need to use different applications, on different shared terminals, located throughout the hospital. They need instant access to their applications and files without searching server directories or folders.

The Solution

The customer already uses a Mifare RFID photo ID badge for physical access control.

They will purchase our Power LogOn software, which includes both the Server's Administrator Card Maker and the Client's terminal logon software, Power LogOn.

Here are some key ways Power LogOn solved the hospital's challenges:

1. **IT Centralized Managed Passwords**

The IT administrator manages all logon passwords, which free up the nurses, doctors, and medical staff from knowing, typing and managing logon usernames and passwords. IT centralized managed entries reduces the cyber threats from social engineering, key loggers, weak, sharing and re-using passwords.

2. **Fast user Terminal Session logon.**

When an employee presents their ID card to the smart card readers, and enter their PIN, they are logged on to a Terminal Services session. No passwords for them to remember or type.

3. **Auto disconnect**

When the employee removes their card from the smart card reader, the terminal session is automatically closed and disconnected. This removes the threat of a hacker exploiting an unattended, open session.

At a later time, and maybe on a different terminal, the employee again present their ID and PIN, and opens a terminal session again. Not having to logon and logoff completely each time has proven to be a great convenience and time saver.

Customer Feedback

Our doctors and nurses were having such trouble remembering their logon information for all the various applications they use. IT Administrators wasted time resetting forgotten passwords.

Since we added Power LogOn, the staff can go from task to task with ease, and IT password reset requests have gone from frequent to occasional. We've received very positive feedback from the medical staff. Power LogOn has provided great relief for them by way of convenience and security. It has also helped IT with HIPAA compliance and meeting the hospital's budget constraints.

We highly recommend Power LogOn and Access Smart for solving the HIPAA MFA cybersecurity requirements.

Power LogOn Evaluation Kits

Access Smart offers Power LogOn evaluation kits for 90-days with a no risk, 100% money back satisfaction guarantee. The kits include:

- A choice between a contact or contactless smart cards system
- Six smartcards
- Two smartcard readers
- The full Power LogOn software
- Six demo licenses, and
- One and a half hours of live installation support

You get everything you need to fully test Power LogOn. Please contact Access Smart, at sales@access-smart.com, or your MSP, to get more information.

Contact Smartcard version



Contactless Smartcard version

