imprivata

CASE STUDY

Medical Center Hospital

Medical Center Hospital uses Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access) to manage vendor privileged access for over 200 unique software applications

mch
Medical Center Hospital
A Member of Medical Center Health System

Medical Center Hospital (MCH) is proud to be the most comprehensive healthcare provider in the Permian Basin. Founded over 70 years ago, they've grown from one facility into a family of healthcare providers delivering a broad range of advanced medical services to the people of Odessa and the surrounding 17 counties.

"Medical Center Hospital now has a standardized method for controlling vendor access and comprehensive, historic audit trails of all vendor activity. It takes a load off of our IT staff, allows us to get better support and delivers fully on the HIPAA requirement to know who is accessing our system and what they're doing while on it. Somebody should have thought of this long before now!"

– Kay Warner, Computer Security Officer Medical Center Hospital

Overview

Vendors were going through MCH's network to support their applications with a wide range of methodologies including modems, VPN accounts, desktop sharing tools, vendor proprietary solutions, and site-to-site networking. These connection types were typically defined by the vendor – whatever they had used with other customers. This variation in connection types created two significant problems for MCH: First, the variety of remote access connections created an overly complex environment that forced the MCH IT staff to become heavily involved

in administering and managing each connection. Secondly, without a standard way of managing remote access, the situation only got more complex as applications, vendors, and support technicians were added to the mix. Finally, there was no common method of tracking and reporting on remote access sessions. If they had the capability at all, audit and reporting differed between connection types and applications. It was impossible to implement a uniform security policy with respect to vendor support access, making HIPAA compliance (with respect to remote access) also very difficult to determine.

Challenges

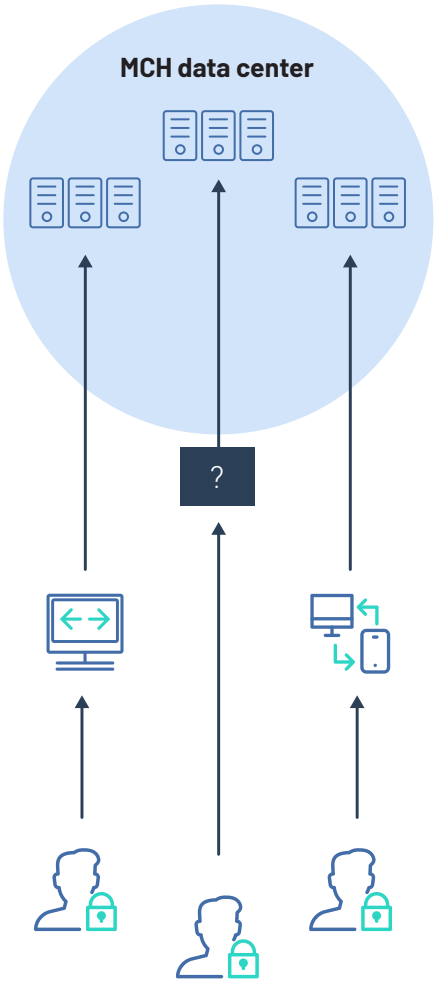
Time-critical support

Application interconnectivity and reliability are essential for keeping patient data flowing between departments to ensure good health care and efficient operations.

Application failure, data corruption, or even slow performance are potentially life-threatening and unacceptable for hospitals trying to maintain high standards of care. A single application outage affects multiple hospital departments – the organization using the application and the others that need the data.

With a small IT staff managing over 200 unique software applications, MCH must rely on software vendors to provide rapid fixes to all problems. This means that, in addition to the typical job of supporting on-site systems and users, the IT staff must also enable remote access by software vendors supporting the hospital's applications. The trick is to provide access for remote support without consuming too much of IT staffs' time and not compromising the security of patient data in the process.

Before Imprivata



Disorganized vendor access was insecure and non-compliant. Logins were shared, audit and accountability were minimal

Data security

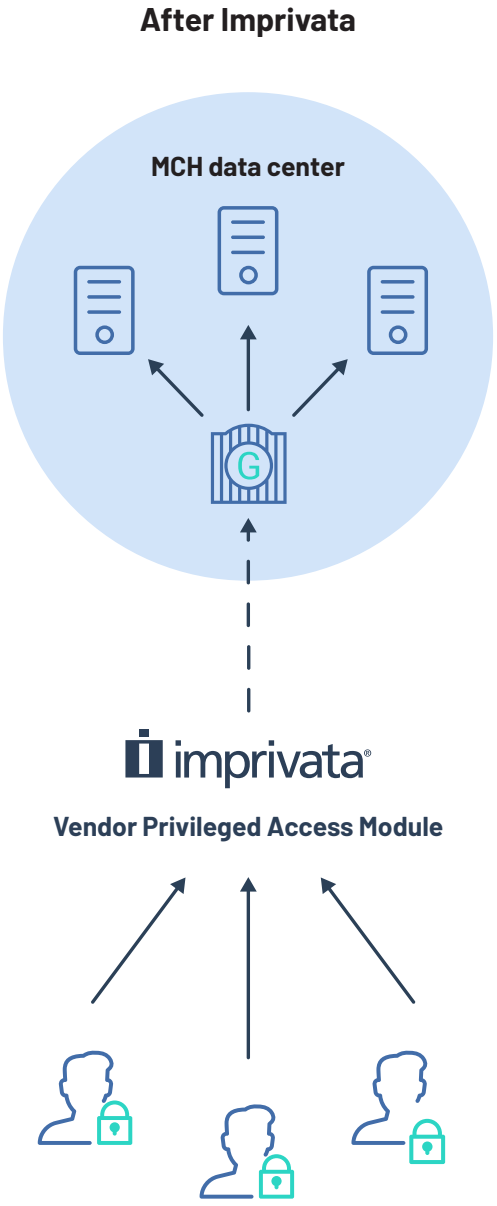
HIPAA requirements have placed healthcare providers in an increasingly controlled environment and have put pressure on hospital IT staff to implement well-defined security policies and systems.

With civil penalties in the tens of thousands of dollars and potential criminal penalties for employees, directors, and officers of covered entities, keeping patient data secure is a clear priority. And, it's not enough to claim to keep the data secure. Systems need to pass rigorous audits in order to prove HIPAA and HITECH compliance.

Results

Imprivata's standardized solution solved the management of vendors on a single platform.

MCH needed to find a way to standardize vendor remote access to reduce the complexity and enable implementation of a robust security policy. Several of MCH's software vendors recently standardized on Imprivata's platform to provide remote support for their clients. Recognizing the power and simplicity of Imprivata Vendor Privileged Access Management, MCH contacted Imprivata about an enterprise version of the product that could be used to manage remote access for all of its vendors. MCH worked with Imprivata to design and deploy the enterprise version of the product, the first systemspecifically designed to enable unified vendor remote access to secure networks. Imprivata Vendor Privileged Access Management standardizes remote access with a system that allows MCH IT staff to easily manage the variety and number of remote support connections needed to keep applications up and running and the hospital operating effectively. Standardization also enables a uniform security policy for remote access.



Using a simple, browser-based interface, the MCH staff was able to strictly define system access for each vendor – server, port, application, files, services, date, time, and more. Once a vendor's access account was set up, the IT staff involvement in administering support connections was minimal.

Shortly after implementing Imprivata Vendor Privileged Access Management, MCH saw a significant reduction in the IT staff's involvement with managing vendor access to their network. The hospital's initial concerns that vendors would be reluctant to shift access were also quickly alleviated.

"Our vendors have been quick to accept and utilize Imprivata Vendor Privileged Access Management. Even our most inflexible vendors recognize Imprivata as a far superior solution to their entrenched and outdated support methodologies."

– Kay Warner

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

VPAM-CS-medical-center-hospital-0124