imprivata

CASE STUDY

# Imprivata Customer Privileged Access Management case study: Veradigm (formerly Allscripts Corporation)

veradigm

**"By converting our customers to Imprivata's remote support network, we were able to save our customers money on their connectivity costs, enhance the reliability of the connection, improve our response and resolution times, all while increasing the security and auditing capability of the customer's systems. Not bad for 15 minutes work!"**

– **Robert Bell,** VP of Product Support Services

## Organization snapshot

Veradigm Corporation (formerly Allscripts) is an enterprise healthcare information technology solutions provider to more than 1,500 major healthcare facilities, including academic medical centers, hospitals with pediatric facilities, and community based hospitals of all sizes. Veradigm's software applications provide workflow and knowledge support to smooth information transfer and patient management between physicians, nurses, managers and other members of the healthcare team.

## Overview

As an end-to-end healthcare solutions provider, Veradigm has an extensive product suite that includes a number of server-based software solutions. With more than 1,500 customers being supported by 1,000 support analysts, Veradigm requires remote diagnostics and maintenance of customer systems to meet cost management and customer satisfaction goals.

Like many companies that support complex applications for a large and diverse client base, Veradigm maintained several remote support solutions and a wide variety of connectivity types. Phone desk, email and chat, and customer initiated web support all required high level of two-party (customer and Veradigm analyst) interaction and were driven by reaction to customer problems instead of proactive management by Veradigm. A wide variety of connectivity types including modems, point-to-point networks, shared desktops and VPNs were expensive, complex and not all secure. The combination of applications and connectivity made it difficult to define and manage process for security, and had no single audit and reporting capability.

## The stakes

Veradigm customers include all of the hospitals on America's Best Hospitals Honor Roll, and nearly half of the more than 100 organizations that have received Magnet Recognition Program status – the highest award an organization can receive for quality of nursing care – use Veradigm solutions. Veradigm customers include Boston Medical center, Cleveland Clinic-Easter Region, The National Institutes of Health, and University of Michigan Hospitals and Health Centers.

# The challenges:

## Key healthcare industry issues

### Application interconnectivity

Hospital departments transfer and share electronic patient data - data that needs to be accessible in real time with views of the information appropriate to the needs of specific departments. Data flow, application interconnectivity and reliability are essential for good health care and efficient operation. Application failure, data corruption, or even slow performance are potentially life threatening and unacceptable for healthcare organizations trying to maintain standards of care. Quality applications and support ensure the continued efficiency, accuracy, and timeliness of information transfer, and all of these lead to better patient outcomes.

### Privacy regulations compliance

Security, privacy and financial regulations have placed health care providers in an increasingly controlled environment. HIPAA is the most influential, but other regulations such as Sarbanes Oxley, EC 95/46, California SB 1386 and others define requirements for security, managing information, and reporting. Protection of data is extended past the healthcare provider to include the vendors supplying software and systems. Failure to meet statutory requirements can lead to disastrous results. In one case, Choicepoint, an information provider to insurance companies, received the largest civil fine in FTC history ($15 million) for compromising the personal information of 145,000 US residents. Compliance with these regulations creates requirements for added process, infrastructure, and application features to enable and enforce the process.

## Veradigm support requirements

### Scalability

Hospital departments transfer and share electronic patient data - data that needs to be accessible in real time with views of the information appropriate to the needs of specific departments. Data flow, application interconnectivity and reliability are essential.

### Security

As a solution provider to HIPAA regulated entities, Veradigm needed to provide solutions that enabled compliance. User control with unique logins for 1,000 employees at 1,500 access points, and audit control to track and record all system access and activities are key features of meeting HIPAA requirements.

### Platform independence

In order to reduce the complexity and cost associated with multiple methods of connectivity, Veradigm needed a single platform to consolidate remote support access and still work with multiple customer platforms. Browser based access with client side components was needed to provide simple, quick, and inexpensive means of establishing and maintaining remote support connections. A consolidated platform also reduces the hardware and software costs associated with managing remote support. Veradigm analysts often use proprietary diagnostic tools to aid in remote application support and speed problem resolution. As customers include more and more operating systems, Veradigm needed a way to control the growing licensing cost of proprietary tools.

## The solution:

With Imprivata Customer Privileged Access Management (formerly SecureLink Customer Connect), Veradigm found a solution that provided the perfect combination of control, flexibility and security. The CPAM server manages, audits and records all of the remote support connections between Veradigm and its customers. Gatekeeper(s), installed on customer servers, enable and define the limits for each remote support connection.

The CPAM server runs on a secure hardened platform of Linux and offers a single point of control for support access to customer systems. Gatekeeper(s) can be installed and set up in minutes providing simple, customer driven access management by defining the hosts, ports, files, directories and applications that Veradigm support analysts are allowed to access.

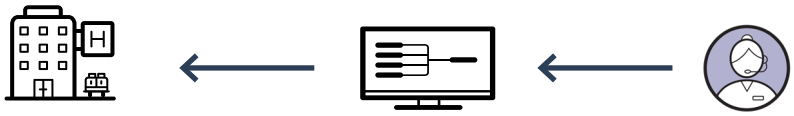
### Veradigm with Imprivata results

Veradigm began to see positive results shortly after rolling out Imprivata Customer Privileged Access Management (CPAM). CPAM's independence gave Veradigm the ability to consolidate its remote support connections on a single platform regardless of the customer's operating system. CPAM ease of use reduced setup costs and improved connectivity response time. As a result, Veradigm saw its support efficiency increase and the cost of connectivity drop by 87%. CPAM's direct, native acccess to customer servers allowed Veradigm' support analysts to use whatever tools they needed to resolve a service issue, eliminating duplication of license fees, further reducing cost and time to problem resolution.

CPAM's ability to let customers strictly define access for each remote support connection, combined with robust audit and reporting functionality allowed both Veradigm and its customers to generate historical audit reports and detail log files capturing who accessed the system, what was done (at the command level), and what tools were used. This satisfied the HIPAA concerns of even the most security conscious customers.

## CPAM features

- Single platform for managing remote support connections to all OS platforms at all customers, reducing connectivity complexity and cost and improving efficiency.
- Direct, native access to the customer server, allowing Veradigm support analysts to use their favorite, proprietary resolution tools without paying additional license fees, increasing effectiveness and decreasing time to resolution.
- Simple, flexible customer managed access controls allowing compliance conscious healthcare providers to restrict access appropriately and increase security.
- Pre-defined controlled access to customer applications reduces time required by customer IT staff to participate in problem resolution, saving cost and improving customer satisfaction. CPAM's ability to allow trusted vendor access without customer involvement meant Veradigm could solve problems without requiring customer involvement.
- Multiple remote connections for a single support session allow Veradigm to apply additional service representatives for faster problem resolution. The CPAM server brokers secure access between the Veradigm technician and the customer's network.
- Detailed audit, reporting and real-time monitoring capability for every remote support session, enabling security process definition and proof of HIPAA compliance.



Remote support module

**The CPAM server brokers secure access between the Veradigm technician and the customer's network.**

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



CPAM-CS-Veradigm-0124