



Addressing HIPAA Security Requirements for Mobile & Wireless Users with CREDANT Mobile Guardian

Business Problem

INTEGRIS Health is Oklahoma's largest not-for-profit healthcare organization, operating twelve major facilities that support over 7510 medical and administrative staff and 450 independent physicians. To fortify their leadership position and to provide higher-quality patient care, INTEGRIS Health uses mobile & wireless technology to access patient records and lab results at the point of care.

However, information resident on mobile devices is not protected by existing network security and poses new threats to the privacy of health information, which is governed by the Health Insurance Portability and Accountability Act (HIPAA) Privacy rule. INTEGRIS Health needed a cost-effective security solution that would protect sensitive information from wrongful disclosure in the event the mobile device was misplaced or stolen.

Business Justification

The primary justification for the investment was to enable physicians to move around freely while leveraging mobile & wireless technology to access information needed to provide higher-quality patient care. However, without the ability to control security for diverse types of mobile & wireless devices, the HIPAA Privacy rule posed a significant barrier to the adoption of mobile & wireless technologies for INTEGRIS Health.

INTEGRIS Health also leverages mobility as a competitive advantage. Independent physicians have the option of choosing which hospital a patient is admitted to and will avoid a hospital that prohibits the technology they want to use to improve patient care and their own personal productivity.

Challenges

To provide managed and secured mobile & wireless services to their users, INTEGRIS Health required a solution that would:

- Control mobile & wireless security enterprise-wide
- Enforce compliance with mobile & wireless security policies with minimal impact to the user experience while satisfying HIPAA regulations
- Reduce cost of compliance
- Protect INTEGRIS Health's networked resources from rogue mobile devices



"INTEGRIS Health leverages mobile solutions to provide business efficiencies, and being Oklahoma's largest not-for-profit health care organization, we must support all types of mobile devices," stated William Woloszyn, RHIA and director of privacy and security for INTEGRIS Health. "CREDANT Mobile Guardian's platform coverage enables us to leverage mobile technology in a secure manner that meets regulatory and industry standards."

Solution

INTEGRIS Health implemented a successful mobile security program using the CREDANT Mobile Guardian security and management software platform. With the CREDANT solution, INTEGRIS Health assured that the privacy of healthcare information is protected, while enabling its physicians and medical staff to safely use mobile devices to access and update patient records and enter orders at the point of care - resulting in reduced errors and delays and higher-quality patient care.

Network Protection

The CREDANT solution enables INTEGRIS Health to control security for mobile & wireless users across diverse computing platforms, including Hewlett Packard iPAQ and Palm. Security policies, enforced on the mobile device by CREDANT Mobile Guardian, mandate the use of a PIN or password to authenticate the user and protect information contained on the device; ensure data confidentiality, even on removable media, with robust data encryption; control connectivity; and automatically delete information from the device if lost or stolen. Security functions are virtually transparent to the user and enabling a physician to reset his or her own PIN/password ensures business continuity.

Reduced Cost of Compliance

Using a web-based interface, CREDANT Mobile Guardian allows INTEGRIS Health to minimize the burden of enforcing compliance with mobile & wireless security policies by centralizing policy administration and automating distribution processes. Integrated with INTEGRIS Health's Microsoft Active Directory, the product allows administrators to establish policy settings and device use based on existing group and user profiles. This eliminates the need to update multiple systems each time a change in employment status is made.

For further information email us at info@codework.com

Visit our website at www.codework.com/credant

