THE CHILDREN'S HOSPITAL

SecureDoc™

Company:	The Children's Hospital - Denver, Colorado
Website:	www.thechildrenshospital.org
Industry:	Healthcare
Challenge:	Protecting confidential patient data on the laptops of an increasingly mobile user community across multiple locations.
Solution:	SecureDoc Enterprise with integration into Denver Children's Hospital

The Challenge:
Protecting Patient Data and Ensuring HIPAA compliance with SecureDoc™

Founded in 1908 in Denver, Colorado, The Children's Hospital is one of the top five children's hospitals in the United States. As a private, not-for-profit pediatric healthcare system, The Children's Hospital is 100-percent dedicated to caring for kids of all ages and stages of growth. That dedication is evident in more than 1,000 pediatric specialists and more than 3,500 full-time employees, and is the main reason that The Children's Hospital is a place parents have come to trust.

As a healthcare provider, The Children's Hospital understood that this trust is not just based on its dedication to providing the best medical attention for the children in its care, but also on its dedication to ensuring all patient records and other sensitive medical information is protected at all times.

Protecting Patient Data Beyond Hospital Walls
With an increasing number of medical staff traveling to extend care beyond the walls of the main campus, two emergency locations, three community-based after-hours care sites, nine specialty care centers, and more than 400 outreach clinics, The Children's Hospital had to be certain that it could protect all data stored on their laptops.

"With more of our clinicians traveling nationally and internationally on a regular basis, we had to be sure that the patient data stored on the laptops that traveled with them was secure," says Andrew Labbo, Privacy and Data Security Officer and Information Security Manager at The Children's Hospital. "The laptops carried by our traveling doctors potentially contain sensitive patient information and so we had to ensure that a lost or stolen laptop would not provide unauthorized access to this highly-confidential data."

The Children's Hospital began researching the best method of protecting data on its laptops. Having looked at the options available, The Children's Hospital decided the only way to ensure all laptop data was protected was full-disk encryption.

"We looked at both whole-disk and file encryption, and found that while whole-disk encryption ensured that no data on a laptop could be accessed by any means," explained Labbo. "With file encryption we could not be certain that all data was protected and would still have to undergo the painful process of notifying all patients in the event of a lost or stolen laptop. Whole-disk encryption also met all HIPAA (Health Insurance Portability and Accountability Act) requirements that call for a mechanism to be put in place to protect data at rest on laptops."

Having decided that full-disk encryption provided the best protection for patient data in transit, The Children's Hospital began testing all available solutions.

The Solution:
SecureDoc: The Right Medicine

"For two months, we researched five different solutions based on numerous criteria," said Labbo. "Of the products we evaluated, only WinMagic's SecureDoc was really capable of meeting all our requirements right out of the box," Labbo continued. "It had the flexibility to integrate with our existing technologies while its versatile installation options meant that busy medical staff would not be disrupted during the installation of the encryption."

The Children's Hospital began a thorough three month pilot. Users included physicians, care providers, executives, and administrative staff. The pilot confirmed that the encryption software met all requirements. "The support staff confirmed that we could fully integrate the encryption software with existing technologies," noted Labbo. "We also confirmed that there would be no disruption associated with adding the encryption layer as users could continue to use their computers while it installed in the background."

Having successfully completed initial testing, Labbo began a larger pilot to test the management software and ensure data would not be lost during installation. "The second pilot lasted six months, and confirmed that once a disk was encrypted, there was little additional management required," commented Labbo. "Both pilots resulted in zero data loss." The pilot also confirmed that the easily scalable encryption software would not only provide the flexible security the busy medical organization required at the present time, but also be able to support future needs moving forward.

With both pilots completed, The Children's Hospital began rolling out the encryption software to additional laptop users. The thorough testing ensured the roll out went exactly as planned. Since the roll out, Labbo's confidence in the software's ability to protect patient data has been further enhanced by personal experience.

"I have SecureDoc on my laptop, and when my hard drive required updating a technician began the process of removing the existing drive and switching the software onto a new drive," commented Labbo. "The technician had experience with encryption solutions in the past, and figured he would not need to remove the software before transferring the data as he could simply bypass the encryption layer," Labbo continued. "Several hours later, the technician came back to me and said he could not bypass the encryption level."

Conclusion:
SecureDoc: The Invisible Cure

The encryption software has met all data protection requirements without compromising the budget of the not-for-profit healthcare provider. In fact, rather than looking at data security as a cost, Labbo prefers to look at it as an excellent investment.

"When you consider the relatively tiny cost of protecting each laptop to the potentially high cost associated with a single user losing their data, it is remarkable to think that every organization is not protecting information in this fashion," said Labbo. "Installing encryption software makes perfect sense from both a data security and an ROI perspective."

Most importantly, the versatile encryption software has enabled The Children's Hospital to protect sensitive medical data without sacrificing the unsurpassed patient care for which it is known. "Once a disk is encrypted, it acts just as it did before it was encrypted," concluded Labbo. "Its almost like SecureDoc isn't even there."

How it Works:
SecureDoc Architecture
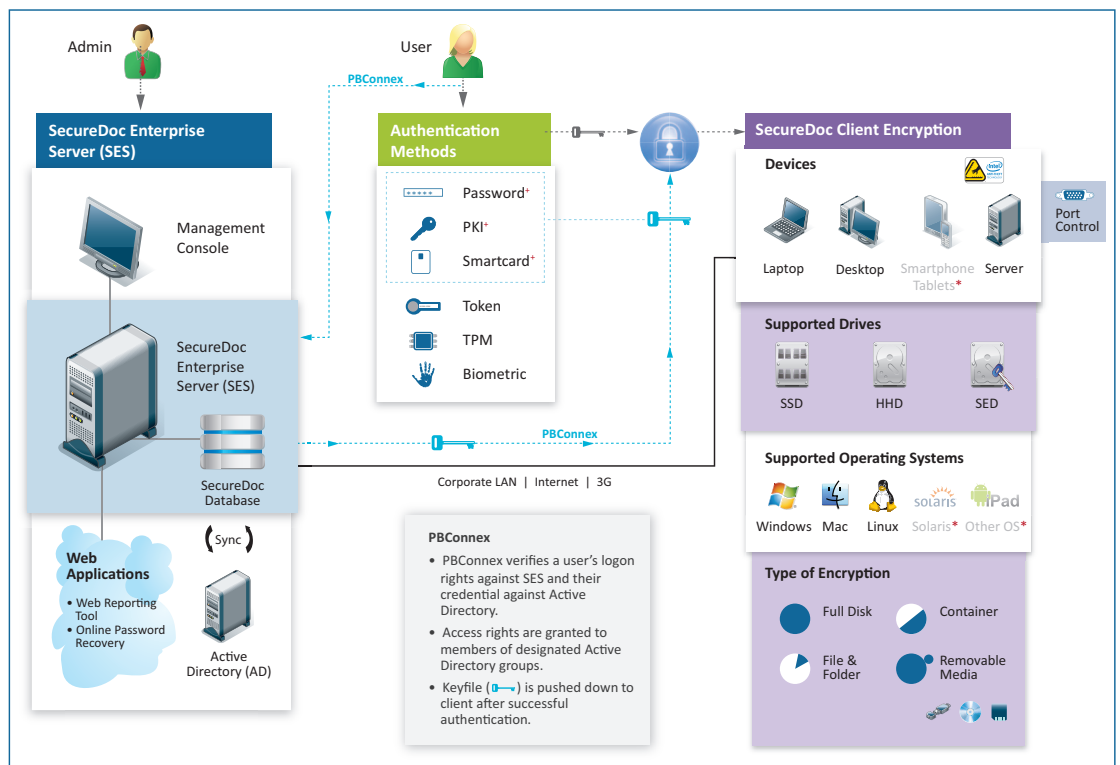
* Available in future release of SecureDoc   + PBConnex Compatible

WinMagic Leading the way to the Next Generation of Full Disk Encryption

WINMAGIC
DATA SECURITY

WinMagic's SecureDoc full-disk encryption solutions make it simple to protect all data on desktops, laptops, tablets and removable media including USB thumb drives, CD/DVDs, and SD Cards. Compatible with Microsoft Windows 7, Vista, XP, and 2000 as well as Mac and Linux platforms, SecureDoc makes it just as easy to centrally manage and use an encrypted device as an unencrypted device including Seagate and Opal self-encrypting drives. WinMagic is trusted by thousands of enterprises and government organizations worldwide to minimize business risks, meet privacy/regulatory compliance requirements, and protect valuable information assets against unauthorized access. With a full complement of professional and customer services, WinMagic supports over three million SecureDoc users in approximately 43 countries. For more information, please visit www.winmagic.com, call 1-888-879-5879 or e-mail us at info@winmagic.com.

CS20110531C