

THE HOSPITAL FOR SICK CHILDREN (SickKids)

Company

The Hospital for Sick Children
(SickKids)

Website

sickkids.ca

Industry

Healthcare

Challenges

Protecting confidential patient data on the laptops of an increasingly mobile user community across multiple locations.

WinMagic Solution

SecureDoc Enterprise with distributed administration and seamless user experience.

For more information on how WinMagic's SecureDoc can protect your data without interrupting user experience contact Sales@winmagic.com. Visit WinMagic.com, or email info@winmagic.com

WinMagic Enables The Hospital for Sick Children to Protect All Data on Mac and Windows Laptops Without Inconveniencing Busy Medical Staff

Wanting to take every possible precaution to protect all data on the laptops and removable media utilized by its medical, research and administrative staff, the Hospital for Sick Children (SickKids), Canada's most research-intensive hospital and the largest centre dedicated to improving children's health, began researching full-disk encryption solutions.

Affiliated with the University of Toronto, SickKids improves the health of children by integrating care, research and learning. SickKids wanted to find a single encryption solution that would protect all data on its laptops as well as make it simple to manage its MXI Security hardware encrypted USB keys without causing any inconvenience to its busy staff.

SickKids researched all available full-disk encryption solutions before narrowing its search down to its top three options. The three solutions selected were then put through more rigorous testing.

"We selected WinMagic Inc's SecureDoc, McAfee Inc's SafeBoot and Utimaco Safeware AG's SafeGuard Device Encryption for a comprehensive Proof of Concept," said Crivianu-Gaita.

As well as scrutinizing each solution for high-level data protection capabilities, the Proof of Concept also included a thorough testing of each solution's ability to protect data on Windows and Mac laptops, ability to integrate with existing security applications, ability to unencrypt data, data recovery capabilities, ability to support security policy protocols, client management and monitoring capabilities, auditing and reporting capabilities and preboot authentication functionality. Only SecureDoc met all SickKids' data security requirements.

"SickKids already had multiple layers of security and numerous security policies in place, so it was critical that the selected full-disk encryption would seamlessly integrate with existing technologies," noted Crivianu-Gaita. "We also wanted a single encryption solution that could protect data on both our Windows and Mac laptops as well as our MXI Security USB keys," Crivianu-Gaita continued. "Testing not only showed that SecureDoc was the only solution that could integrate with our complex environment, but it also confirmed that SecureDoc would enable our administrators to centrally manage laptops as well as removable media from a single central console."

SickKids was also pleased to find that SecureDoc's pre-boot capabilities meant that it would not interfere with patient care.

"As SecureDoc integrates with all devices at pre-boot users do not have to deal with a second log-in screen," commented Crivianu-Gaita. "This transparency means that as far as users are concerned their laptops operate exactly the same with the encryption installed as they do without encryption." With the Proof of Concept completed, SickKids began a two-month pilot to ensure the installation and deployment of SecureDoc would run smoothly.

The pilot involved 25 laptops used by physicians, administrators and researchers. Testing confirmed that SecureDoc would make it simple for SickKids to centrally deploy enterprise-class 'always-on' full-disk encryption to all staff. As the solution installs in the background without any real degradation in laptop