



ENTRUST



North York General Hospital uses advanced technology to enhance patient-centric care



IDENTOS

North York General Hospital (NYGH) is one of Canada's leading community academic hospitals, offering a wide range of acute, ambulatory and long-term care services across its three facilities. Established in 1968 in the north central region of Toronto, the hospital currently has over 5,000 staff, physicians and volunteers.

NYGH is the first acute care hospital in Canada to be presented with the prestigious Davies Award of Excellence, in recognition for its eCare initiative; an innovative hospital-wide information technology transformation project. NYGH joins an elite group of only 50 hospitals in the world to receive the coveted award since its creation in 1994 by the renowned Health Information Management Systems Society (HIMSS).

TECHNOLOGY AS AN ENABLER

The use of leading-edge technology to advance its excellence in integrated patient-centered care is further demonstrated by a recent initiative to facilitate the secure exchange of information between physicians, healthcare staff and patients. Given the highly sensitive nature of the communications, the project includes a foundational layer that utilizes cryptography – and the secure management of cryptographic keys – to ensure that all interactions remain confidential and completely unintelligible for everyone other than the message sender and legitimate recipient.

LEARN MORE AT [ENTRUST.COM/HSM](https://www.entrust.com/hsm)



North York General Hospital

The initiative focused on bringing medical staff and patients closer together through the deployment of enhanced online communications. In-person consultations would be supplemented with exchanges using PCs and mobile devices; enabling more timely and convenient interactions.

The hospital's traditional way of securing its infrastructure had been through the use of firewalls to create rigid division between internal and external traffic. The need to embrace users located outside of the hospital's boundaries - as required by the new project - dictated an enhancement of NYGH's traditional security measures.

DESIGNING FOR GROWTH, FLEXIBILITY AND PRIVACY

The underlying design principle was that all communications, from any device or location, had to be completely private and secure. It also was imperative that the chosen security strategy didn't restrict the growth of participants in the program as it gained popularity. In addition to providing robust protection, the architecture had to inherently ensure that there was sufficient flexibility to enable the use of a wide range of devices - including patient-owned mobile phones, medical appliances and ultimately IoT components - without locking the hospital into a narrow security paradigm.

As an important part of its due diligence, the hospital researched the best practices of other highly respected healthcare organizations. Having evaluated many different approaches, a decision was taken to implement an encryption-based strategy with a robust root of trust.

PARTNERING TO PROTECT

NYGH selected IDENTOS, a global provider of encryption services and solutions, and an Entrust technology partner, to provide the security platform needed to run the service. The IDENTOS encryption-as-a-service subscription platform is integrated with Entrust nShield® Connect hardware security modules (HSMs) to protect and manage the cryptographic keys within a hardened device.

NYGH utilizes the IDENTOS and Entrust solution to ensure data is protected both in motion and at rest. As information is exchanged between clinicians and patients, nShield HSMs maintain a root of trust for the encryption keys used by the IDENTOS solution in a secure hardware environment - as required by industry security best practices. The nShield HSM enhances the security of the software-based solution.

nShield is fully compliant with the FIPS 140-2 standard defined by the U.S. National Institute of Standards and Technology (NIST) and the Canadian Security Establishment (CSE).



North York General Hospital

« **Behind the scenes technology platforms are enabling healthcare providers to achieve significant improvements in patient care, efficiency, and safety delivering care. The IDENTOS and Entrust security platform is a key part of our growing mobile strategy, enabling us to offer the convenience demanded by today's mobile-savvy users and simultaneously further expand our admired culture of patient-centered care.** »

- Sumon Acharjee, CIO, North York General Hospital

Applicable in both the United States and Canada, FIPS 140-2 is the most widely adopted security benchmark for cryptographic solutions in government and commercial enterprises. Entrust nShield HSMs generate the Advanced Encryption Standard (AES) encryption keys required by NIST that are used by the IDENTOS data encryption platform.

The IDENTOS solution enables additional features and functionality to be added to the hospital's environment without requiring changes to the underlying encryption solution, irrespective of the volumes of data being transferred. The automation of many administrative tasks, such as reporting and encryption key

back-ups, enabled by the IDENTOS/Entrust solution minimizes operational costs and reduces human error.

Sumon Acharjee, NYGH's CIO and driving force behind the project, summarized, "Behind the scenes technology platforms are enabling healthcare providers to achieve significant improvements in patient care, efficiency, and safety delivering care. The IDENTOS and Entrust security platform is a key part of our growing mobile strategy, enabling us to offer the convenience demanded by today's mobile-savvy users and simultaneously further expand our admired culture of patient-centered care."



North York General Hospital

ENTRUST AND IDENTOS PROVIDE PLATFORM FOR GROWTH

Business need

- Provide secure connectivity for external users
 - Utilize technology to help drive patient-centered culture
 - Implement solution that doesn't restrict growth and flexibility
- Technology need

Technology need

- End-to-end protection of traffic
- Identify encryption solution that adheres to multiple compliance standards
- Utilize hardware-based encryption rather than a software-oriented approach

Solution

- IDENTOS Encryption as a Service integrated with Entrust nShield HSMs

Result

- Traffic that is leveraging the platform – including PII and PHI – is always secure
- Effective application of technology brings staff and patients closer together
- Foundation created for future growth and feature expansion

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.



Learn more at

entrust.com/HSM



ENTRUST