ノースヨーク総合病院は、高度テクノロジーを使用して、患者中心のケアを強化しています

ノースヨーク総合病院（NYGH）は、カナダの有数の地域教育病院の1つであり、3つの施設で、救急、外来、長期の幅広いケアサービスを提供しています。この病院は1968年にトロントの中北部に設立され、現在5,000人を超えるスタッフ、医師、ボランティアがいます。

NYGHは、病院全体の革新的な情報技術変革プロジェクトであるeCareイニシアチブが評価され、名誉あるDavies Award of Excellenceを受賞した、カナダで最初の救急病院です。NYGHは有名な健康情報管理システム協会（HIMSS）によって1994年に設立されて以来、この切望される賞を受賞した、世界でわずか50の病院からなるエリートグループに加わっています。

イネーブラーとしてのテクノロジー

患者中心の統合型ケアにおける卓越性を向上させるために最先端技術が使用されていることは、医師、医療スタッフ、患者の間の安全な情報交換を支援する最近のイニシアチブによってさらに実証されています。コミュニケーションの機密性が非常に高いため、このプロジェクトには、暗号化を利用した基盤レイヤーと暗号化鍵の安全な管理が含まれており、すべてのやり取りはメッセージの送信者と正当な受信者以外のすべての人には機密に保たれ、全く理解できないようになっています。

ノースヨーク総合病院

このイニシアチブでは、強化されたオンラインコミュニケーションの展開を通して医療スタッフと患者の距離を縮めることに重点を置かれました。対面での診療は、PCやモバイルデバイスを使用した情報交換で補完されるため、よりタイムリーで便利なやり取りが可能です。

病院のインフラストラクチャを保護する従来の方法は、ファイアウォールを使用して内部トラフィックと外部トラフィックを厳密に分割することでした。病院の境界外にいるユーザーを受け入れる必要性が新しいプロジェクトで求められ、NYGHの従来のセキュリティ対策の強化が決定されました。

成長、柔軟性、プライバシー保護のための設計

基本的な設計原則は、デバイスや場所を問わず、すべてのコミュニケーションを完全にプライベートで安全にする必要があるというものでした。また、選択したセキュリティ戦略が人気を博したため、プログラムの参加者の成長を制限しないことも不可欠でした。アーキテクチャは堅牢な保護を提供することに加え、本質的に、病院を狭いセキュリティの枠組みに閉じ込めることなく、患者が所有する携帯電話、医療機器、最終的にはIoTコンポーネントを含む、幅広いデバイスの使用を可能にする十分な柔軟性を確保する必要がありました。

デューデリジェンスの重要な部分として、病院は他の高く評価されている医療機関のベストプラクティスを調査しました。多くの異なるアプローチを評価した結果、強固な信頼ルートを備えた暗号化ベースの戦略を実装することが決定されました。

保護のためのパートナー提携

NYGHは、暗号化サービスとソリューションのグローバルプロバイダーであるIDENTOSと、Entrustテクノロジーパートナーを選択して、サービスの実行に必要なセキュリティプラットフォームを提供しました。IDENTOSのサービスとしての暗号化サブスクリプションプラットフォームは、Entrust nShield®Connectハードウェアセキュリティモジュール（HSM）と統合され、強化されたデバイス内の暗号化鍵を保護・管理します。

NYGHは、IDENTOSおよびEntrustソリューションを使用して、データが使用中と保存中のときの両方で保護されるようにします。臨床医と患者の間で情報交換が行われるとき、nShield HSMは、業界のセキュリティベストプラクティスで求められるように、安全なハードウェア環境でIDENTOSソリューションによって使用される暗号化鍵の信頼ルートを維持します。nShield HSMは、ソフトウェアベースのソリューションのセキュリティを強化します。

nShieldは、米国国立標準技術研究所（NIST）およびカナダ通信保安局（CSE）によって定義された、FIPS140-2標準に完全に準拠しています。

ノースヨーク総合病院

舞台裏のテクノロジープラットフォームにより、医療機関は、患者のケア、効率、ケア提供における安全性の大幅な改善を実現できます。IDENTOSとEntrustのセキュリティプラットフォームは、成長を続けるモバイル戦略の重要な部分であり、今日のモバイルに精通したユーザーが求める利便性を提供すると同時に、患者中心のケアという称賛される文化をさらに拡大することができます。

– Sumon Acharjee、ノースヨーク総合病院CIO

FIPS 140-2は、米国とカナダで適用可能であり、政府および民間企業の暗号化ソリューションに最も広く採用されているセキュリティベンチマークです。Entrust nShield HSMは、IDENTOSデータ暗号化プラットフォームで使用されるNISTに必要なAES（Advanced Encryption Standard）暗号化鍵を生成します。

IDENTOSソリューションを使用すると、転送されるデータの量にかかわらず、基盤となる暗号化ソリューションを変更する必要なく、病院の環境に追加の機能を加えることができます。IDENTOS／Entrustソリューションによって可能になる、レポートや暗号化鍵のバックアップなどの多くの管理タスクの自動化により、運用コストが最小限に抑えられ、人的エラーが減少します。

NYGHのCIOであり、プロジェクトの推進力であるSumon Acharjee氏は、次のように要約しています。「舞台裏のテクノロジープラットフォームにより、医療機関は、患者のケア、効率、ケア提供における安全性の大幅な改善を実現できます。IDENTOSとEntrustのセキュリティプラットフォームは、成長を続けるモバイル戦略の重要な部分であり、今日のモバイルに精通したユーザーが求める利便性を提供すると同時に、患者中心のケアという称賛される文化をさらに拡大することができます。」

ノースヨーク総合病院

ENTRUST とIDENTOSは成長のためのプラットフォームを提供

ビジネスニーズ

- 外部ユーザーに安全な接続を提供する
- テクノロジーを利用して、患者中心の文化を推進する
- テクノロジーに必要な成長と柔軟性を制限しないソリューションを実装する

技術的ニーズ

- トラフィックのエンドツーエンドの保護
- 複数のコンプライアンス基準に準拠する暗号化ソリューションを特定する
- ソフトウェアベースのアプローチではなく、ハードウェアベースの暗号化を利用する

ソリューション

- Entrust nShield HSMと統合されたサービスとしてのIDENTOS暗号化

結果

- プラットフォームを利用しているトラフィック（PII、PHIを含む）は常に安全です
- テクノロジーの効果的な適用により、スタッフと患者がより緊密になります
- 将来の成長と機能拡張のために構築された基盤

ENTRUSTについて

Entrustは、信頼性の高い本人認証、決済、データ保護を可能にすることにより、世界の動きを安全に維持します。今日、人々はこれまで以上に、国境を越えた移動、買い物、電子政府サービスへのアクセス、企業ネットワークへのログインといったさまざまな場面で、シームレスで安全なユーザー体験を求めています。Entrustは、これらすべてのインタラクションに対応した、他では見られない広範なデジタルセキュリティおよび資格情報発行用ソリューションを提供しています。2,500名以上の従業員とグローバルパートナーのネットワークを備え、150か国以上における顧客から支持されているため、世界における多くの委託組織から信頼を得ていることは不思議ではありません。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

ENTRUST

お問い合わせ：
HSMinfo@entrust.com