Introduction
Healthcare Information Exchanges (HIE) provide the capability to electronically move clinical information among different healthcare organization like hospitals, physician offices, pharmacies, and health insurance companies. HIEs are quickly emerging since they facilitate access to clinical data allowing healthcare professionals a more efficient and simple way to access patient data.

This movement to electronic access of such pertinent data for healthcare affiliates has many benefits for all parties involved—physicians, patients, health insurance companies and hospitals.

➤ Physicians can easily exchange information between secondary care takers or additional providers while saving time and money doing so electronically.

➤ Healthcare insurance companies can reduce expenses with paper and ink, avoiding duplicate tests, scanning, printing, faxing of documents, and physical mailing of associated documents.

➤ Pharmacies can reduce cost and time by electronically receiving prescriptions reducing paper costs, time and dollars spent.

➤ And finally, patients will benefit in many ways since there will be a centralized location of all their medical information and can be easily accessed by any necessary healthcare professionals, speeding up critical diagnoses and treatments.

Studies in the industry indicate that a doctor’s practice spends over $10,000 per year in exchanging just one patient’s healthcare data. Federal and State Governments are still scrambling to finalize legislation for these exchanges, but what is clear to all parties involved is the crucial need for security of this sensitive data.

Security Considerations
With different types of networks and different ways to exchange and store information, several security policies and security methods must be implemented to ensure integrity of these networks and meet future compliance needs.

With these different factors coming into play, healthcare providers must meet many challenges in securing data moving across these HIE networks including:

➤ Security Management - With patients being able to opt-in and opt out at different levels, a security management system must be implemented to manage the different layers of security required for different patients. Many current HIEs already have policies in place where patients can choose what types of information in their medical records should be shared—this will require the implantation of different security policies.

➤ Interoperability - Interoperability between all different participating parties including different hospitals, private practices, pharmacies, physician offices, ambulatory centers, and specialty offices. HIEs must use security vendors whose products work seamless together with one another.
Internal and External Access Control - With different participants opting in to the HIE as well as different size organizations, different levels of access will be required for the many different parties in the system. This will require access control but more importantly, a customized approach to access control. For example, a large hospital may use a hardware security module for the large amounts of data entering and leaving their building where an ambulatory care center may only need USB authentication for data received and sent out. Providers must be able to have a scalable solution for access control as well as a management system to manage who can access the system as well as control the different levels of administrator access.

Central Storage - Patient information and transaction integrity going hand in hand with access control. Business operations without bogging down their system. Information, while those not authorized, can still perform only authorized users may gain access to this sensitive encrypted and protected. With the proper system in place, patient information and critical to their operations remain accessed by unauthorized users. By deploying encryption solutions, users of the HIE network can be assured that the applications, servers, and databases containing patient information and critical to their operations remain encrypted and protected. With the proper system in place, only authorized users may gain access to this sensitive information, while those not authorized, can still perform business operations without bogging down their system. Protecting these records against potential hacks.

User Authentication - Going hand in hand with access control is identity management. Employees involved in an HIE must have a way to prove who they are before accessing such sensitive data. This can also be done through vsmart cards, tokens or certificate-based authentication, which will also require a central management system to implement policies on identity management.

Patient Information and Transaction Integrity - Data integrity is extremely significant for not only securing that sensitive data but also to use encryption to ensure message authenticity and delivery of messages and patient data to the proper destination. Using encrypted networks can secure data and ensure the authenticity and proper delivery of patient records.

Central Storage - Lastly, many of the HIEs will have a central repository of patient data stored in one location. Providers must make sure that those repositories are not accessed by unauthorized users. By deploying encryption solutions, users of the HIE network can be assured that the applications, servers, and databases containing patient information and critical to their operations remain encrypted and protected. With the proper system in place, only authorized users may gain access to this sensitive information, while those not authorized, can still perform business operations without bogging down their system. Protecting these records against potential hacks.

HIE Network Security Offerings

- Transaction and Application Security
- Key Management and Data Protection
- Secure Network Communications
- User Authentication

Data Protection Solution Offerings for HIE Network Security

There are several areas in HIE’s where security is a critical factor—security of issued certificates and other stored data, encryption of data moving along the exchange, and authentication of users onto the exchange. Gemalto can address all of these issues with its Identity and Data Protection products. By providing multi-factor authentication technologies, hardware security modules (HSMs), high speed encryptors (HSEs), and data encryption solutions, Gemalto can secure HIEs at all necessary junctures.

Transaction and Application Security Hardware

Security Modules (HSMs) provide reliable protection for applications, transactions, identities, and information assets for HIEs. Compared to software based alternatives, only HSMs provide the utmost security and highest performing solutions for the protection of cryptographic keys, the provision of encryption, decryption, authentication and digital signing services. Gemalto offers a broad portfolio of HSM products to meet the needs of any size healthcare organization. Gemalto’s SafeNet HSM solutions can be used at larger locations in healthcare exchanges like hospitals and healthcare organizations while token-based technologies could serve smaller offices and buildings like pharmacies and smaller physician practices.

Key Management and Data Protection

The strongest, most effective security solutions rely on cryptographic processes at their core. Key management ensures the secure storage and protection of private keys integral to the security of a PKI. If someone other than the actual holder of the key gains access to a private key, the PKI security model is compromised. Therefore, in a PKI environment, particularly one critical to HIE business processes, it is essential that private keys be guarded with a reliable key management solution. Gemalto’s SafeNet Identity and Data Protection solutions focus on sensitive patient records and data—ensuring information is protected at every moment—when it is created by a healthcare employee on a company laptop, shared with a HIE network partner, stored in an database, processed by an application, and accessed by a medical employee on a mobile device.

High Speed Encryption between Parties

Since critical information will be exchanged back and forth between hospitals, physicians, pharmacies, and insurance organizations, encryption and protection of these communications is vital. Gemalto’s SafeNet High Speed Encryptors from Gemalto provide the fastest and easiest way to integrate robust, FIPS-certified network security to protect mission-critical data. Encrypting all data, including video, voice and metadata as it crosses the network, SafeNet High Speed Encryptors offer maximum bandwidth efficiency ideal for the HIEs, as well as disaster recovery sites, site to site networks, data centers, and storage area networks on premises, in the cloud and in transit.
User Authentication

The final piece in securing Healthcare Information Exchanges includes the authentication of users onto the exchange. SafeNet’s strong authentication solutions offer the broadest range of authentication methods and form factors, allowing organizations to address multiple use cases and risk levels from a single authentication backend. Organizations can apply one-time-password (OTP) or certificate-based authentication through a variety of FIPS 140-2 Level 1 validated hardware and software form factors. These include smart cards and USB tokens, as well as OTP apps that transform any mobile device into an OTP token, eliminating reliance on USB ports and ideal for practitioners working off premises or from multiple different clinics. Providing a single point of management, SafeNet’s solutions enable enforcing consistent access controls to the HIE as well as other IT resources, securing single-sign on applications, standard enterprise applications (email, spreadsheets, etc.) as well local and remote (VPN) access to EHRs and other healthcare systems. Plus, hospitals and physicians can leverage the same strong authentication solution to comply with the DEA’s EPCS regulation.

1. The user is authenticated into the HIE using a strong authentication token.
2. The patient information is sent over to the HIE through a secure Ethernet pipe.
3. Patient information and applications are encrypted in the HIE database and servers without bogging down critical operations.
4. Sensitive certificates are issued and protected, as well as electronic documents signed using hardware-based encryption.

SafeNet Identity and Data Protection products offer the most-complete, standards-based security options for Healthcare Information Exchanges (HIEs), and equip all parties involved in HIEs with the agility they need to adapt to change and act on opportunity.
The SafeNet HIE Security Advantage

SafeNet solutions can equip all parties involved in HIEs with the agility they need to adapt to change and act on opportunity. SafeNet’s wide-range of products for all areas of information security networks provide for a saleable solution depending on the size and location of each entity participating in the HIE.

SafeNet delivers persistent protection of information at critical points in its lifecycle, wherever and however that information gets used. SafeNet delivers these comprehensive capabilities:

- Strong authentication and identity management solutions that protect identities for users and servers
- Industry-validated, hardware-based encryption platforms that protect transactions, ensure data integrity, and maintain an audit trail
- Data encryption solutions that protect and maintain ownership of data throughout its lifecycle—from the data center across the network and into the cloud
- High-performance communications encryption solutions that persistently protect information ensure control beyond location or boundary, streamlines operations, and reduces compliance cost

About Gemalto’s SafeNet Identity and Data Protection Solutions

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions—from the edge to the core. Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com
Follow Us: data-protection.safenet-inc.com

GEMALTO.COM