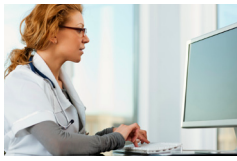

10
The Top 10 things you should know
about HEALTHCARE IT SECURITY
SafeNet
The Foundation of Information Security



Maintaining the security of patient data is a complex proposition that affects every employee of a healthcare facility, every area of its IT system, and all vendors, partners, and insurers that work with the healthcare provider.

While many facilities are working toward achieving full compliance with HIPAA, HITECH, and other privacy regulations, there are a variety of factors to consider that go beyond compliance issues to address the overall risk to your facility. With that in mind, we present 10 things you should know about healthcare IT security:

10

Protected Health Information (PHI) is a prime target.

PHI records typically contain sensitive data such as name, date of birth, Social Security number, insurance information, and medical history. So it's no surprise that healthcare data theft is the fastest growing criminal enterprise today — more than financial, education, or corporate HR records.

9

Healthcare breaches are increasing.

In the past 12 months, nearly one in five healthcare facilities have reported a breach that required notification. This represents a 6% increase over the previous year. Even more disconcerting, recent surveys put the total percentage of healthcare facilities that have had at least one data breach at 84%.

8

Most breaches come from inside.

66% of breaches are the result of unauthorized or inadvertent actions of employees. From misdirected emails and faxes to lost or stolen laptops, sensitive information can be exposed at any point in the process. Even if the intentions are not malicious, data can find its way into an unprotected environment.

7

The costs can be astronomical.

In 2006, the industry average reconciliation cost of a breach was approximately $180 per record. By 2008, that number had grown 11% to $200, and the costs continue to rise. A single breach of 5,000 records can easily cost a healthcare company in excess of $1,000,000. Beyond the direct costs of addressing a breach, failures in patient data security can lead to a loss of trust among patients, stakeholders, and the community, along with damage to the organization's reputation, a loss of patient and revenue streams, and an increase in liability.

6

Online information needs 24/7 protection.

As more medical records are going online, and hospital networks are sharing this data among doctors, patients, and insurers on the Internet, it's imperative to control who has access to the information and secure the application itself from data breaches.



5

The rules are always changing.

From HIPAA in 1996 to HITECH in 2009, federal and state legislation is increasing the demands on healthcare IT systems to protect patient data and report breaches — and fines are increasing. So, taking action now will maximize your security budget.

4

Sensitive information is everywhere.

Healthcare providers and practitioners have embraced mobile computing through smartphones, PDAs, and laptops, creating new vulnerabilities in healthcare IT systems. Yet, even handwritten documents need to be protected from the wrong eyes.

3

Time is of the essence.

Medicare and Medicaid reimbursements up to $44,000 will be available from 2011 through 2014 to help facilities comply with the HITECH Act. However, starting in 2015, penalties on reimbursements will begin for facilities that have not achieved compliance.

2

If it's not encrypted, you're not protected.

Whether in the database, in use by the furthest end user, or at any point in between, unencrypted data is vulnerable to theft or misuse. The presence or absence of encryption can also be a deciding factor in determining liability in the event of a breach.

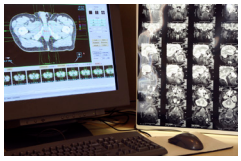
1

You, personally, can be held liable.

As the focus on patient data safety continues to increase, regulations are shifting to add personal liability to corporate liability, opening the doors to fines — and even jail time — for those responsible for safeguarding data.

While all of this may sound intimidating, and it should, there's only one thing you need to know to address this entire Top 10 list — SafeNet. Simplified, scalable patient data protection.





Simplify your patient data security with the most complete, centralized, and end-to-end solution in healthcare.

SafeNet provides a flexible, centralized solution to secure your patient data records and health history, billing account information, intellectual property (e.g., medical and pharmaceutical patents), and any other data or transaction information your organization needs to safeguard.

By using an Information Lifecycle Protection (ILP) framework that combines encryption, access policies, key management, content security, and authentication, SafeNet's Data Protection allows healthcare organizations to align IT strategies with future business growth through a comprehensive, intelligent, persistent, and extensible approach. All critical encryption and key management requirements are centrally implemented, eliminating the need to invest in disparate systems from different vendors.

In a single, comprehensive platform, healthcare organizations can ensure regulatory compliance and secure local as well as remote access to critical applications and ePHI. SafeNet ILP provides end-to-end protection for identities, transactions, and applications — helping to secure operational efficiencies.

Maximum performance for uninterrupted access
All the components comprising SafeNet ILP are designed for superior encryption performance to ensure their seamless integration with your business processes and patients' experience. Offloading and centralizing data encryption processing to highly specialized hardware appliances delivers performance levels that support the most demanding processing environments with ease.

- Multi-factor strong authentication with hardware security modules (HSMs) protect identities for users, and control physical and logical access to data, building stakeholder trust in your organization.
- Industry-validated, hardware-based encryption and key storage platforms protect transactions and applications, ensure data integrity (including the process of moving from paper to digital), and maintain an audit trail.
- Data encryption and control solutions protect and maintain ownership of data throughout its lifecycle — from the data center to the endpoint (including mobile devices used by physicians, clinicians, and administrators) and into the cloud.
- High-performance communications encryption solutions persistently protect information, ensure control beyond location or boundary, streamline operations, facilitate disaster recovery, and reduce compliance costs.

Streamlined implementation helps meet deadlines and avoid fines
SafeNet solutions are designed for fast and easy integration into existing IT infrastructure. With out-of-the-box connectors and centralized deployment capabilities, SafeNet dramatically reduces implementation time and cost to ensure deadlines are met and fines avoided.

Modular flexibility and scalability meet specific compliance and data security needs
Evolving security threats call for an evolutionary solution. SafeNet provides a comprehensive foundation of security modules within a common, integrated framework that allows you to select and add the security controls that fit your unique strategic data protection requirements. This integrated approach enables you to protect every data asset today — and in the future — with the highest degree of assurance and the lowest cost of ownership.

Get a free security audit

Protect your data, your patients' privacy, and your peace of mind. Contact SafeNet **1-877-817-0107** or visit **www.safenet-inc.com** today to arrange a free, no-obligation security audit of your IT system and discover how you can reduce your risk and be cost-effectively compliant.

SafeNet
The Foundation of Information Security