THALES

THE TOP 10 THINGS YOU **SHOULD** KNOW *about* HEALTHCARE IT 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, HITRUST, 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. This information is highly sought after, so it is no surprise that the Breach Level Index shows identity theft was the most prevalent data breach type in 2018.

09

Healthcare faces the most security threats.

According to the Breach Level Index, healthcare companies experienced the greatest amount of security events in H1 2018 amongst all the industries.

08

Most breaches come from inside.

73% of breaches in the healthcare industry are the result of unauthorized or inadvertent actions of employees. From privilege misuse, through 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.

07

The costs can be astronomical.

The Ponemon Institute's 2019 Cost of Data Breach Study shows that the healthcare industry pays an average of $429 per breached record, the highest cost per record across industries. 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.

06

Online information needs 24/7 protection.

Online information needs 24/7 protection. As medical records and prescriptions 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 applications and secure the appropriate access points with strong two-factor authentication and to ensure that the data is encrypted both in motion and at rest. The DEA's EPCS regulation, for example, requires practitioners to re-authenticate to EHR applications using strong two-factor authentication when issuing e-prescriptions for controlled substances.

05

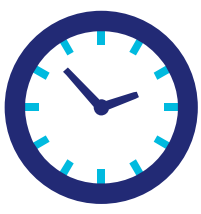
The rules are always changing.

From HIPAA in 1996 to GDPR in 2018, 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 let you meet state and nationwide deadlines and enjoy federal incentive programs, while maximizing your security budget.

04

Sensitive information is everywhere.

Healthcare providers and practitioners have embraced mobile computing through smartphones, PDAs, and laptops, creating new vulnerabilities in healthcare IT systems. This has resulted in even more data being at risk of exposure as copies can be made with ease and backups are stored beyond the confines of the traditional data center, in virtual environments and in the cloud.



03

Time is of the essence.

Starting in 2015, hospitals that do no use electronic health records are subject to financial penalties. Conversely, to qualify for Medicare or Medicaid EHR financial incentives, Hospitals and CAHs must demonstrate 'Meaningful Use' of Electronic Health records as set out in Stage 2 and Stage 3 objectives. EPCS deadlines vary by state, with some compliance deadlines already in effect.

02

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

Whether in a 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.

01

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—Thales. Simplified, scalable patient data protection.

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

Thales 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 a centralized identity and data protection framework that combines encryption, access policies, key management, and authentication, Thales's Identity and Data Protection (IDP) Solutions allow 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. Gemalto IDP provides end-toend protection for identities, transactions, and applications—helping to secure operational efficiencies.

Maximum performance for uninterrupted access

All the components comprising Thales IDP 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.
- **Multi-factor strong authentication with hardware tokens or software tokens** (OTP apps) helps control access to a range of medical systems, and enables complying with the DEA's EPCS regulation. The same tokens can be used not only to re-authenticate to EHR systems when issuing eRx's for controlled substances, but also to secure remote access to EHRs for practitioners working off premises.
- **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

Thales IDP solutions are designed for fast and easy integration into existing IT infrastructure. With out-of-the-box connectors and integrations, and centralized deployment capabilities, Thales 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. Thales 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.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com