SOPHOS

Regulations and Standards: Where Encryption Applies

By **Dave Shackleford**, Founder of Voodoo Security

There are many regulations worldwide relating to the protection of private and sensitive data. Some focus on protection of specific industry information, others on proper disclosure of data loss incidents and general privacy attributes. The first section of this paper describes the types of data under regulation and basic best practices for implementing appropriate encryption technologies. The second section reviews data privacy regulation (financial and medical regulations as well as private individual data regulations), how encryption applies to them and basic best practices for those applications.

Overview

Most of today's standards and compliance regulations are concerned largely with private data protection at rest, during transactions, and traversing network connections. Some regulations simply require particular technologies for compliance, but encryption can be employed for all of them to satisfy the protection requirements. By determining what data you are required to protect, and by locating the data at rest and in transit and implementing the appropriate encryption technologies, you can significantly improve your overall security posture while complying with any number of data security and privacy regulations.

Rules and regulations are changing globally, from the European Union Data Protection Reform to U.S. state data breach laws. A good example of a regulation that's changed dramatically is the U.S. Health Insurance Portability and Accountability Act (HIPAA). It was substantially enhanced by the new provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and it now levies fines for sensitive data exposure. In the U.S., more and more states have also tightened their data privacy laws. As of 2014, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands all have data protection and privacy laws on the books. In addition, most countries across the rest of the world have their own specific data protection laws and regulations.

The first section of this paper describes the types of data under regulation as well as basic best practices for implementing appropriate encryption technologies. The next section includes data privacy regulation overviews (financial and medical regulations as well as private individual data regulations), how encryption applies to them and basic best practices for those applications.

This updated paper explores changes in the information security regulatory landscape over the last several years, especially those related to data protection and encryption. Some have gotten more stringent with actual fines and penalties being levied, while some totally new ones have emerged with more on the way. This paper is an update to one originally published in 2007 by Utimaco and the SANS Institute.[1]

Changes since 2007

Several countries are looking into law and statute updates currently, for example a major planned update to European Union data protection laws is coming in late 2014. The biggest changes to personal data protection laws have occurred in the United States. The most tangible changes in U.S. law are those to HIPAA. HIPAA was updated in 2009 with the HITECH Act, which created a number of interim rules for better defining protected healthcare data, affected parties, breach disclosure, penalties and enforcement of penalties against Covered Entities and Business Associates.

In 2013, a large and sweeping piece of legislation known as the HIPAA "Omnibus Rule" was passed, making a number of changes primarily focused on providing clarity in expected protection of data as well as solidifying the penalties for non-compliance. For example, Section 164.306(c) of the HIPAA Security Rule now more clearly indicates that Covered Entities and Business Associates must review and modify security measures as needed to ensure the continued provision of "reasonable and appropriate" protection of Electronic Protected Health Information (ePHI).

Under the HIPAA Privacy Rule, Business Associates are now directly liable for impermissible uses and disclosures, as well as numerous other violations. Another major change in the new rules modifies the Breach Notification Rule that was in place (interim) from HITECH in 2009. In the new rule, the impermissible use or disclosure of Protected Health Information (i.e. a violation of the HIPAA Privacy Rule) is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the Protected Health Information has been comprised. In other words, if a proper risk assessment has been conducted and the data is properly encrypted, there may not be a need for breach disclosure.

Penalties for HIPAA violations have also been made much more stringent. There are now four (4) clear categories of violation specified with penalties for each violation:

- Did Not Know: $100-$50,000 per violation
- Reasonable Cause: $1,000-$50,000 per violation
- Willful Neglect-Corrected: $10,000-$50,000 per violation
- Willful Neglect-Not Corrected: $50,000 per violation

In addition, fines of up to $1.5 million can be levied for violations of an identical provision in a given calendar year, as determined by the Department of Health and Human Services (HHS). This gives HHS the leeway to potentially levy much larger amounts if multiple different types of violations are found.

Many of the general principles relating to the U.S. HIPAA/HITECH regulations often also apply with regional and cultural differences in other international jurisdictions.

Several state data protection laws in the United States have also been updated or created since 2007, with a clearer emphasis on best practices for securing data including the use of encryption. In particular, Massachusetts and Nevada both specifically mention encryption in their state laws from 2010.

The Nevada data protection law has a number of specific requirements related to data protection. First, if the "data collector" organization handles payment card data, the law requires compliance with the current version of the Payment Card Industry Data Security Standard (PCI DSS). Second, transmission of data or movement of a "data storage device" containing sensitive information "...beyond the logical or physical controls of the data collector, its data storage contractor or, if the data storage device is used by or is a component of a multifunctional device, a person who assumes the obligation of the data collector to protect personal information, unless the data collector uses encryption to ensure the security of the information."[2]

The Massachusetts data protection law also specifically requires the use of encryption. Under section 17.04, "Computer System Security Requirements," the law requires "encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly" as well as "encryption of all personal information stored on laptops or other portable devices."[3]

Additionally, in 2012, the state of California also started requiring companies and state agencies to submit data breach disclosures to the state Attorney General for review. The state's 2012 data breach report reveals that encryption use would have saved 1.4 million California residents from having their sensitive information exposed.[4] In fact, the Attorney General strongly recommends the use of encryption technologies to safeguard data in this report.

The Payment Card Industry Data Security Standard (PCI DSS) has seen several updates, with the release of version 3.0 in 2013. In 2008, the PCI Council published a document articulating what merchants should and should not do with regard to payment card data storage. It states that merchants should "...use strong cryptography to render unreadable cardholder data that you store, and use other layered security technologies to minimize the risk of exploits by criminals."[5] In the latest version of the PCI DSS, as well as the Payment Application Data Security Standard (PA-DSS), encryption is explicitly required in numerous sections of the standards, with very prescriptive specifications. "Strong cryptography" is defined in a separate PCI glossary (with 112 bits minimum key length and states acceptable algorithms), with a reference to a detailed guide from NIST (NIST Special Publication 800-57).[6]

A number of countries and international regions are currently implementing new privacy and data protection laws. The Privacy Amendment (Enhancing Privacy Protection) Act of 2012 was passed by the Australian parliament in November 2012 and became law in March 2014. The new Act contains significant reforms to the Privacy Act, including replacing the National Privacy Principles for the private sector and Information Privacy Principles for Commonwealth and Australian Capital Territory Government agencies with a single consolidated set of principles referred to as the Australian Privacy Principles (APPs).

The new Act also significantly strengthens the powers of the Australian Information Commissioner to conduct investigations and ensure compliance with the amended Privacy Act. The Australian government has published a guide to information security that should be evaluated for all organizations and entities responsible for protecting sensitive data when investigating a breach. Encryption is explicitly mentioned with questions on key management, coverage and so on.[7]

In addition, a new General Data Protection Regulation reform proposal is in progress within the European Union that will define a Union-wide data protection framework to replace the existing patchwork of country-specific legislation. It is intended to strengthen the privacy rights of EU citizens, restore confidence in online activities and better protect customer data by requiring companies to adopt new data protection processes and controls. The penalties in case of a data breach are proposed to range up to a seven figure sum or several percent of global revenue.

Examples of Data Breaches and Fines

There are many examples of data breaches in the news today. The December 2013 breach of payment card information at Target, for example, has affected up to 70 million individuals.[8] In the past, few organizations suffering breaches have experienced significant long-term ramifications, including loss of business and stiff penalties and fines. However, that may be changing:

- In June 2012, a hard drive containing unencrypted Electronic Protected Health Information (ePHI) was stolen in Alaska from an employee of the Alaska Department of Health and Human Services (DHHS), leading to a $1.7 million fine.[9]
- In October 2012, the UK Information Commissioner's Office (ICO) fined the Stoke-on-Trent City Council GBP 120,000 after sensitive data was sent unencrypted in emails.[10]
- A Massachusetts healthcare organization paid $1.5 million to HHS in September 2012.[11]
- WellPoint Inc. paid HHS $1.7 million for failing to implement security safeguards and controls in July 2013.[12]
- In December 2013, Spain fined Google EUR 900,000 for violating EU data protection laws.[13]
- In February 2014, a Puerto Rican insurance company was fined $6.8 million for HIPAA violations.[14]

With the pace of breaches and penalties accelerating, organizations need to get a handle on security controls for sensitive data in their environments. What follows is a simple primer on data types, areas of security focus and how to start or advance a sound data protection program that meets best practices.

Data Definitions

Although there are many distinct types of data to consider, most fall into these broad categories:

- **Financial data**: The types of financial data are numerous, but commonly include credit card account numbers and track data, banking account numbers and associated financial information, and a variety of credit-related data on individuals and businesses. Several regulatory standards, particularly Sarbanes-Oxley in the Unites States, are concerned with financial reporting data for public companies.
- **Protected Health Information**: Sensitive patient health data, which can include insurance-related data, actual medical information, and patient personal data such as Social Security numbers, addresses, and other sensitive information that should not be publicly available.
- **Private individual data**: Social Security numbers, addresses and phone numbers, and other personally identifiable data that could potentially be used for identity theft and other illicit activity.
- **Merchant data**: Primary account number (PAN), also referred to as "account number" is a unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

- **Military and government data**: Data specific to government programs, particularly those related to military departments and operations are carefully regulated.
- **Confidential/sensitive business data**: Data that has to be kept secret including trade secrets, research and business intelligence data, management reports, customer information, sales data, etc. falls into this category.

Data at rest is data commonly located on desktops and laptops, in databases and on file servers. In addition, subsets of data can often be found in log files, application files, configuration files, and many other places. Today, with the prolific use of external storage devices such as USB disks plus cloud-based systems and platforms, this data could easily be located outside the traditional boundaries of most organizations' controlled data center environments.

Data in transit is commonly delineated into two primary categories – data moving across public or "untrusted" networks such as the Internet, and data moving within the confines of private networks such as corporate Local Area Networks (LANs). A related concept is data in use, which refers to data that is being processed. One example is a bank balance transaction update, which needs to occur in a secure tamper-proof environment.

Best Practices for Data Privacy Compliance

Most organizations today have some degree of responsibility for protecting sensitive data. Implementing a sound protection strategy can be a daunting task – where do you start? What follows is a simple, step-by-step approach to protect the sensitive data in your environment.

1. Assess your organizational structure to understand where your business is being conducted.
2. Know what rules apply to your organization, particularly when you have international locations.
3. Know what you need to encrypt. Any sensitive data types that need to be protected for regulatory compliance or to comply with internal policies and standards can be strong candidates for encryption. If you have a data classification policy, encrypt the most sensitive or critical category (or the top two most sensitive categories).
4. Understand data format: [3digits][dash][2digits][dash][4digits]. A number of techniques and technologies exist for searching for strings and data patterns, including the use of regular expressions. An excellent site that describes the use of regular expressions in detail can be found at http://www.regular-expressions.info/tutorial.html.
5. Locate data at rest that is housed in systems across the enterprise, including (but not limited to):
    - **Databases**: Data at rest is most commonly found in the form of relational databases, where data is stored in logical tables that can be linked to other related tables of information. Each row of a database comprises a single record made up of multiple distinct pieces of information, and each column of a database table represents an attribute of that record. For example, each row may represent a patient health record, and columns may include name, address, last doctor visit, social security number, etc.

Determine which databases and database tables contain the private information, then narrow this to the specific columns that contain the data that needs to be protected. This can be accomplished using specific SQL queries or by using built-in database management tools. In some cases, entire tables or databases may be sensitive, but it is more likely that certain columns are considered more sensitive than others.

- **File shares and large-scale storage (such as a Storage Area Network, or SAN)**: Data residing on these systems can take any number of formats, including documents and word processor files, application-specific configuration or output files and spreadsheets.
- **Email systems**: Email content may be stored in databases or file shares, but the use of email for sending and receiving sensitive data is common and content is often stored on centralized mail servers, as well as cached locally on desktop systems and e-mail backup archives.
- **Individual desktop and laptop systems, as well as PDAs, smartphones, and removable media**: Data stored locally, either in an office environment or on systems that are often in the field. PDAs and other small personal computing devices may have Flash-based removable storage that contains data.
- **Backup media**: Often overlooked when locating sensitive data, backup tapes and other media can contain significant amounts of sensitive data and may be stored in remote locations for disaster recovery and business continuity purposes.
- **Cloud Storage**: Cloud-based storage solutions, either dedicated service offerings for storage or connected storage to Infrastructure-as-a-Service (IaaS) environments, are increasingly popular with enterprises. Depending on the configuration of the cloud storage environment and visibility consumers have into these cloud environments, discovery and protection of sensitive data stored here may be challenging.
- **Hybrid Storage systems**: Hybrid storage that incorporates traditional disks coupled with flash-based storage can make data discovery and protection somewhat more challenging.

It is also critical to assess the end-of-life status of devices and storage media and completely destroy or sanitize hard drives and other storage media prior to resale of such IT equipment.

6. Locate data in motion, traversing network channels both within and outside organizations by:
   - Assessing the data trajectory: This is the path that the sensitive data traverses through your network.
   - Gaining visibility into the network traffic itself: The goal is to understand the protocols and applications involved in actually encapsulating the content. This may be accomplished with sniffers or other network traffic capture and monitoring software. Application-layer inspection is paramount to determine whether sensitive data is being transmitted and whether it is encrypted properly.

- Determining whether certain network devices are storing sensitive data or related information. Each network device that the data traverses may have varying levels of data storage in structures such as log files. Do not overlook these when assessing the trajectory of sensitive data throughout a network.
- Inspecting specific gateway devices such as mail servers and proxies, as they may have different storage and communications methods than traditional network devices such as routers and firewalls.

7. Once sensitive data has been identified in a specific location, there are four primary options for protection:
   - Eradication: This is not likely to be a practical option. Total removal of data is difficult to achieve, particularly in real-time. Additionally, there are often valid business reasons for storing some sensitive data.
   - Segmentation: Segmenting sensitive data at a storage or network level can be useful and successful at limiting data exposure and meeting compliance requirements.
   - Obfuscation: Modifying the stored format of data so that it is not easily readable or accessible. This option is often employed for transaction-related information such as credit card numbers (i.e., full payment card track data may be sent to a processor at the time of use, but the merchant may only store the last four digits of the card number and must obfuscate the rest). One-way hashes and tokenization are often used to obfuscate sensitive data or remove it entirely from usage scenarios by replacing it with token codes.
   - Encryption: Widely considered the most effective means of protection. With proper key management and application, encryption can be used to protect database columns or tables, files on servers, entire communication channels, hard drives and email messages.
8. Align yourself with a reputable partner. Encryption is not a technology that lends itself to in-house development. Work with reputable vendors whose products meet your particular requirements.
9. Create a sound, manageable set of encryption policies that can be adhered to and that meet organizational requirements. Policy points should include:
   - A test plan for implementing encryption solutions. Choose a sample group for implementation and ensure that the technology works properly.
   - Use of strong encryption with a well-known and community-tested encryption algorithm. Typically, 128-bit keys and larger are considered strong.
   - Auditing a sampling of systems after rollout begins to ensure data is properly encrypted and that there are no issues with deployment.
   - Strong key management processes.
   - Role-based access controls in conjunction with encryption and key management implementation. Encryption can be used to effectively guarantee confidentiality of data for distinct groups in your organization (e.g., the Sales team cannot read the HR data).
   - Routine audits to ensure that policies are being followed and the system is working properly.

Conclusion

Most of today's standards and compliance regulations are largely concerned with the protection of private data at rest, during transactions, and while traversing network connections. Some of these regulations make specific recommendations or require particular technologies for compliance. Encryption can be employed for all of them to satisfy the protection requirements. By determining what data you are required to protect, locating the data at rest and in transit and implementing the appropriate encryption technologies, you can significantly improve your overall security posture while complying with any number of data privacy regulations as well.

Sample regulations with supporting encryption requirements and best practices.

- PAYMENT CARD INDUSTRY DATA SECURITY STANDARD 3.0 (PCI DSS 3.0)
- GRAMM-LEACH-BLILEY ACT (GLBA)
- SARBANES-OXLEY ACT (SOX)
- BASEL II ACCORD
- 8TH COMPANY LAW DIRECTIVE (EURO-SOX)
- FINANCIAL INSTRUMENTS AND EXCHANGE ACT OF 2006
- HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
- HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT (2009)
- FDA TITLE 21 CFR PART 11 (1997)
- 95/46/EC EUROPEAN UNION (EU) DIRECTIVE
- BUNDESDATENSCHUTZGESETZ (BDSG)
- NEVADA NRS 603A AND MASSACHUSETTS 201 CMR 17.00
- PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)
- DATA PROTECTION ACT 19987 (DPA)
- PERSONAL INFORMATION PROTECTION LAW (PIPL) OF 2003
- CALIFORNIA SENATE BILL 1386 (SB 1386)

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD v3.0 (PCI DSS 3.0)

FOCUS: Protection of payment card data and related consumer/business details during processing, transmission, and storage

SCOPE: Global - specified by MasterCard and Visa as well as other payment card brands

PENALTIES: Significant fines for non-compliance

Requirements	Crypto Discussion	Best Practices
PCI DSS requirements are **only** applicable if a Primary Account Number (PAN) or specific track data is stored, processed, or transmitted. **DSS Req. 3: Protect stored cardholder data** Full magnetic stripe data, CVV2 and CVC2 data for card verification, and PIN blocks cannot to be stored at any time. Stored data can include Primary Account Numbers (PANs), Cardholder name, expiration date, and service codes.	PAN data can be rendered unreadable by hashing or truncating the numbers, as well as employing strong cryptography with proper key management. Disk encryption must show logical separation of accounts managing or accessing the encryption vs. user accounts.	Any solution must be both robust and manageable to meet DSS requirements. This includes: › Strong key generation › Secure key storage and distribution › Periodic changing of keys › Proper destruction of keys › Protection of key integrity Key management and lifecycle, where applicable, is emphasized heavily in PCI DSS v3. SSL/TLS and IPSec (WPA/WPA2 for wireless) should be used to transmit sensitive data across public networks (such as the Internet).
DSS Req. 4: Encrypt transmission of cardholder data across open, public networks Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.	Email encryption of payment card data is explicitly mentioned if email is necessary for transmitting PAN data. Any PAN data sent via email should be encrypted prior to transmission.	

GRAMM-LEACH-BLILEY ACT (GLBA)

FOCUS: Protection of private data in the financial services industry

SCOPE: U.S. - Banking and financial services industry

PENALTIES: Significant fines and potential criminal charges

Requirements	Crypto Discussion	Best Practices
Sections 505 in Subtitle A and 521 under Subtitle B describe specific agencies and types of organizations mandated with protecting the security and confidentiality of consumer nonpublic personal information (NPI). Organizations include US national and Federal branches of foreign banks, member banks of the Federal Reserve System, credit unions, and any association insured by the Federal Deposit Insurance Corporation (FDIC).	While not specifically mandated, database, folder, full-disk and transport VPN / transport encryption all apply.	Choose encryption type (Full-disk or file/folder) based on usage: › Full-disk or file/folder on mobile devices › Folder encryption is best used on servers where only certain directories contain sensitive information › Encrypt all sensitive information in databases › Encrypted virtual private network (VPN) tunnels using SSL or IPSec Implementing additional measures such as: › Key management and other administrative processes › Physical safeguards for cryptographic key storage
§ 6801(a): It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. **§ 6801(b)**:...each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information;(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."	Nonpublic personal information (NPPI) can be protected at rest or in transit with any number of different encryption solutions: › Full-disk and file/folder encryption › Database encryption › Encrypt over Virtual Private Networks (VPN) Consider encryption your last line of protection against "anticipated threats." Traditional defense and protection measures will still apply for proper defense-in-depth, but encryption will always serve as the last, and possibly most effective, measure of protection.	

SARBANES-OXLEY ACT (SOX)

FOCUS: Protection of sensitive data related to financial reporting in public companies. Provide guidance for public companies in designing and reporting on the controls in place for protecting financial information

SCOPE: Global - All industries

PENALTIES: Civil and Criminal for exposure of data or fraudulent behavior

Requirements (COBIT 4.1)	Crypto Discussion	Best Practices
DS5.7 Protection of Security Technology: Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.	Accepted frameworks for use with SOX are COSO and COBIT.	**General**: › Remote management using secure encrypted channels (SSH, SSL, IPSec) › Encrypt security device log data at rest and in transit **Technologies**: › Dedicated key storage devices and applications › Key management applications that allow provisioning of keys and separation of duties with proper access controls, as well as auditing capabilities **Procedures**: › Use of encryption technologies, › Allocation of access rights to keys based on roles › Key recovery procedures › Specific guidance on handling of keys in various environments Policy should be fluid enough to respond to evolving encryption standards, and should directly relate to data classification schemas.
DS5.8 Cryptographic Key Management: Determine that policies and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.	Proper key management is essential as key compromise undermines overall system security.	
DS5.11 Exchange of Sensitive Data: Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt, and non-repudiation of origin.	Implement encryption technologies for network connections that carry financial reporting data and related sensitive information. This could be VPN technology or dedicated encryption gateways that encrypt "on-the-fly."	
DS11.6 Security Requirements for Data Management: Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, organizational security policy and regulatory requirements.	Mandatory encryption for financial reporting data and other related sensitive information at rest, in transit, and during processing must become part of the data's lifecycle.	

BASEL II ACCORD

FOCUS: International standard for operational and financial risk management for banking institutions

SCOPE: Global - Banking

PENALTIES: Requirements to reserve greater levels of operating capital, less favorable pricing in financial markets

Requirements	Crypto Discussion	Best Practices
There are three "pillars" of risk management under Basel II. The first pillar is concerned with financial and liquidity risk, describing how banks and financial institutions can prepare for credit, operational, and market-driven risks. The second and third pillars discuss regulator interaction with financial institutions, numerous other types of risk, and responsible disclosure.	Although no technical controls are specified for data protection, corporate oversight, internal control review, and loss events are explained thoroughly. Basel II is entirely focused on the implementation of a sound operational risk management strategy. Any number of types of risk may be addressed, including the risk of computer attacks and penetration, loss of sensitive data, employee theft, and other possible attacks against data integrity.	The incorporation of a holistic information security strategy, focused on risk management, is the appropriate best practice to follow for Basel II compliance. This will include areas such as the following: › Security policy and procedures › Perimeter protection mechanisms › Data protection such as encryption › Data integrity measures like hashing and digital signatures › Appropriate access control and authorization controls

8TH COMPANY LAW DIRECTIVE (EURO-SOX)

FOCUS: Protection of sensitive data related to financial reporting in public

SCOPE: EU - Banking and financial services industry

PENALTIES: Criminal (including incarceration) and civil, significant potential fines

Requirements	Crypto Discussion	Best Practices
The European Union determined that better governance and financial controls legislation was needed to improve investor confidence in European businesses. EU adopted a series of directives between 2003 and 2006, which went into law by the end of 2008 as the 8th Company Law Directive. Key directives that directly relate to internal financial and IT controls for financial data include: › The European Union Financial Services Action Plan (FSAP) › The 4th directive Annual Accounts of specific type of companies › The 7th directive Consolidated accounts › The 8th Company Law Directive on Statutory Audit › The 8th Company Law Directive and Corporate Governance › The 8th Company Law Directive Committees and Interpretations Several of these are directly focused on professional ethics, independence and objectivity in reporting and auditing, auditing standards, audit reporting, and auditors' liability. Additionally, assessment of internal controls and review of these controls is also discussed to some extent.	The program is somewhat similar in nature to the U.S. Sarbanes-Oxley Act. Mandatory encryption for financial reporting data and other related sensitive information at rest, in transit, and during processing must become part of the data's lifecycle. Implement encryption technologies for network connections that carry financial reporting data and related sensitive information. This could be VPN technology or dedicated encryption gateways that encrypt "on-the-fly."	**General**: › Remote management using secure encrypted channels (SSH, SSL, IPSec) › Encrypt security device log data at rest and in transit **Technologies**: › Dedicated key storage devices and applications › Key management applications that allow provisioning of keys and separation of duties with proper access controls and audit trail information (assignment of keys, recovery keys, etc.) **Procedures**: › Use of encryption technologies › Allocation of access rights to keys based on roles › Key recovery procedures › Specific guidance on handling of keys in various environments Policy should be fluid enough to respond to evolving encryption standards, and should directly relate to data classification schemas.

FINANCIAL INSTRUMENTS AND EXCHANGE ACT OF 2006

FOCUS: Protection of sensitive data related to financial reporting in public. Enhancement of internal controls over financial reporting data

SCOPE: Japan - Banking and financial services industry

PENALTIES: Yes

Requirements	Crypto Discussion	Best Practices
The Financial Instruments and Exchange Act of 2006 became law in Japan in 2008, and is often referred to as "J-SOX". Companies are ensuring compliance by documenting internal controls, both IT-focused and financial and ensuring security safeguards are in place for all financial reporting data. Definition of the maximum criminal penalties against various market frauds and expanding the scope of penalties against criminal and fraudulent behavior is also included in the law.	Encryption falls under the security safeguards category, which applies to data at rest and in transit. While not specifically mentioned, all major encryption technologies for both endpoints (full-disk, file/folder) and network connections (VPN access) are in scope.	**General**: › Remote management using secure encrypted channels (SSH, SSL, IPSec) › Encrypt security device log data at rest and in transit **Technologies**: › Dedicated key storage devices and applications › Key management applications that allow provisioning of keys and separation of duties with proper access controls **Procedures**: › Use of encryption technologies › Allocation of access rights to keys based on roles › Key recovery procedures › Specific guidance on handling of keys in various environments Policy should be fluid enough to respond to evolving encryption standards, and should directly relate to data classification schemas.

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)

FOCUS: Protection of electronic patient healthcare data and information

SCOPE: U.S. - Required of all designated 'covered entities' and business associates

PENALTIES: Enforced via HITECH and Omnibus Rule of 2013

Requirements	Crypto Discussion	Best Practices
HIPAA addresses the implementation of administrative, physical, and technical safeguards for Electronic Protected Heath Information (ePHI). **Section 164.306 Security Standards** Covered entities must: › Ensure the confidentiality, integrity and availability of all electronic protected health information they create, receive, maintain, or transmit › Protect against any reasonably anticipated threats to the security or integrity of such information › Protect against any reasonably anticipated uses or disclosures of such information that are not permitted **Section 164.312 Technical Safeguards** 164.312(a) (2) (iv) Implement a mechanism to encrypt and decrypt Electronic Protected Health Information. 164.312(e)(2)(ii) Implement a mechanism to encrypt Electronic Protected Health Information whenever deemed appropriate **(for transmission security)**	HIPAA provides specific recommendations for access control, risk analysis, data disposal and re-use, and data encryption. Policy and documentation requirements are also detailed. Encryption technologies can assist with ensuring the confidentiality of patient health information, and also serve as a strong measure of protection against today's commonly anticipated threats such as unauthorized access, modification, and disclosure. Encryption, though not specifically mandated, is listed as an addressable technical measure that can be implemented for data at rest and in transit.	**For data at rest**: › Employ strong full-disk or folder-level encryption for all ePHI › For ePHI in databases, implement full database or column-level encryption › Implement sound key management procedures and processes that accommodate proper separation of duties and least-privilege for users and applications › Employ data integrity measures that hash or digitally sign all electronically stored ePHI data **For data in transit**: › Implement a Virtual Private Network (VPN) using either IPSec or SSL for all remote systems that may need to transmit ePHI › Implement encryption for all systems and users that may need to send ePHI via email

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT (2009)

FOCUS: Protection of electronic patient healthcare data and information

SCOPE: U.S. - Required of all designated 'covered entities' and business associates

PENALTIES: Yes, up to $1.5 million

Requirements	Crypto Discussion	Best Practices
The HITECH Act specifies that encryption can and should be used for protection of patient health information. For data in motion, HITECH states: "Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2." For data at rest, HITECH states: "Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices." Furthermore, strong encryption is the only mechanism for data protection that obviates the need for data breach notification in the case of compromise.	The HITECH Act simply seeks to provide reinforcement for HIPAA in the form of clarity regarding cryptography use (and expectations for ePHI), as well as expectations and information related to data breach notification for business associates and covered entities. HITECH adheres to the fundamental principles laid out for HIPAA - encryption of data at rest and in motion, with emphasis on full-disk encryption and encryption via SSL and messaging applications, is critical to privacy and protection of personal health information. HITECH, however, includes more specificity regarding fines and penalties, and also dictates more specifically when, and how, data breach notification should take place when ePHI is involved. If encryption is in use, no data breach notification is required by law.	**Authenticity**: › Employ digital signatures for all communications and messages covered under the mandate. This may include email, documents, electronic voice messages, etc. **Integrity**: › Use a recognized hashing algorithm such as MD5 or SHA-1 to create hash fingerprints of all stored data. This hash data should be considered sensitive, as well, and stored appropriately to avoid tampering or unauthorized access **Confidentiality**: › Use strong encryption for data at rest and in transit to prevent unauthorized access and exposure. This may include VPN technology, database or file encryption, full-disk encryption, etc.

/ FDA TITLE 21 CFR PART 11 (1997)

FOCUS: Defines the criteria whereby electronic records and signatures would be considered trustworthy and reliable

SCOPE: Global - Any drug makers and other FDA-regulated industries doing business in the U.S.

PENALTIES: Yes, financial and criminal

Requirements	Crypto Discussion	Best Practices
The mandate includes information about controls, audits, documentation, and other validation needed to be considered compliant. Section 11.10 specifically mandates controls that should be in place to protect the integrity and security of electronic records and signatures on closed systems with limited access. These include validation, archival protection, access controls to limit exposure to data to authorized individuals, and written policies. Section 11.30 specifies controls for more open systems, including document encryption and digital signature standards.	Encryption technologies can assist with ensuring the confidentiality of data covered by the mandate. This may include any type of stored information relevant to drug manufacturing and distribution, as well as other FDA-regulated businesses. In addition, other related technologies can be used to provide non-repudiation and integrity measures as well.	**Authenticity**: › Employ digital signatures for all communications and messages covered under the mandate. This may include email, documents, electronic voice messages, etc. **Integrity**: › Use a recognized hashing algorithm such as MD5 or SHA-1 to create hash fingerprints of all stored data. This hash data should be considered sensitive, as well, and stored appropriately to avoid tampering or unauthorized access **Confidentiality**: › Use strong encryption for data at rest and in transit to prevent unauthorized access and exposure. This may include VPN technology, database or file encryption, full-disk encryption, etc.

95/46/EC EUROPEAN UNION (EU) DIRECTIVE

FOCUS: General protection of individual's private information

SCOPE: EU - All industries and governments

PENALTIES: None specifically stated

Requirements	Crypto Discussion	Best Practices
Personal data can only be processed when three basic conditions are met: › When the person is informed of the processing ('transparency') › When the processing is for a legitimate purpose › When the data processed is "in proportion" to the actual purpose. Brief mention is made directing responsible parties ('processors') to take care in securing the data and ensuring confidentiality. **Article 17: Security of Processing** Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.	This directive, one of the older and more well-established regulations related to protection of personal/private data, defines personal data extremely broadly. Basically anything that could be linked back to identify an individual is deemed to form personal data. Although the language used is not technology-specific, both data at rest and in transit is referenced. The directive states that any responsible entity must take appropriate measures to protect individuals' personal data. Encryption certainly falls under this category.	Encryption solutions of all types, including full-disk and file/folder encryption for data at rest and SSL/IPSec VPNs for data in transit, could be implemented to prevent unauthorized access to or disclosure of sensitive data.

BUNDESDATENSCHUTZGESETZ (BDSG)

FOCUS: General protection of individual's private information

SCOPE: Germany - All industries and governments

PENALTIES: Various penalties for misuse

Requirements	Crypto Discussion	Best Practices
Germany's Federal Data Protection Act, (Bundesdatenschutzgesetz, or BDSG), has been revised several times over the last four decades, and exists to protect the collection and dissemination of personal data by public and private organizations. The regulation deals with a broad range of use cases and penalties for misuse.	No specific technologies are mentioned in the regulation. However, it does require appointment of a data protection officer in certain organizations that process data, and the document's Annex specifies the need for access controls, protection of data at rest, authorization, and other security-specific measures.	**General best practices for encryption would apply**: › Strong access controls; including VPN technology for remote access and data in transit › Use of whole-database or column-level encryption for any private data stored in databases › Use of full-disk or folder-level encryption stored on disk › Key management tools and procedures should be implemented for access controls to encrypted resources › Appropriate encryption policies should be in place

Nevada NRS 603A & Massachusetts 201 CMR 17.00

FOCUS: General protection of individual's private information

SCOPE: U.S. - All organizations with customers and/or employees in the U.S. states of Nevada or Massachusetts

PENALTIES: Yes

Requirements	Crypto Discussion	Best Practices
For organizations with customers and/or employees in the U.S. states of Nevada or Massachusetts, these bills require disclosure of a security breach where there is a reasonable belief that unauthorized access to unencrypted personal information has occurred. The bills specifically apply to data stored on computers. Any sensitive data not encrypted is subject to the disclosure provisions. A breach is defined as unauthorized access to or acquisition of computerized data that potentially compromises the security, confidentiality, or integrity of personal information.	201 CMR 17.00 states that a security program should include the following: › Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly. › Encryption of all personal information stored on laptops or other portable devices. NRS 603A mentions encryption in the context of data that is recognizable as "personal information". Without encryption, the data is presumed to be recognizable as personal data.	**Encrypt the following data, at a minimum**: › Social security number › Driver's license number or state Identification Card number › Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account Any of the aforementioned data, when connected with an individual's first name or initial and last name, is considered to be sensitive personal data. **General best practices for encryption would apply**: › Use of VPN technology for sending private data in transit › Use of whole-database or column-level encryption for any private data stored in databases › Use of full-disk or folder-level encryption stored on disk › Key management tools and procedures should be implemented for access controls to encrypted resources › Appropriate encryption policies should be in place

PERSONAL INFORMATION PROTECTION & ELECTRONIC DOCUMENTS ACT (PIPEDA)

FOCUS: Protection of personal and private data under certain circumstances

SCOPE: Canada - Electronic Commerce

PENALTIES: Federal mediation and 'negative' press releases

Requirements	Crypto Discussion	Best Practices
Support more secure electronic commerce by requiring protection of personal and private data that is collected, used, or disclosed in certain circumstances. Protection will include physical measures like locks, organizational measures like security clearances, and technical measures like passwords and encryption. A bill (Bill C-475) was proposed in 2013 to update PIPEDA with more specific protections and accountability requirements for organizations handling personal data, but was defeated in January of 2014.	No specific technology is mandatory, but it applies in all areas where protected data travels and resides.	**General best practices for encryption would apply**: › Use of VPN technology for sending private data in transit › Use of whole-database or column-level encryption for any private data stored in databases › Use of full-disk or folder-level encryption stored on disk › Key management tools and procedures should be implemented for access controls to encrypted resources › Appropriate encryption policies should be in place

DATA PROTECTION ACT 1998 (DPA)

FOCUS: Handling of personal information

SCOPE: UK - All industries and business

PENALTIES: Criminal and civil fines, data forfeiture

Requirements	Crypto Discussion	Best Practices
UK Parliament mandate dealing with information about proper disclosure, rights of access to information, transmission and processing, and proper protective measures.	No specific technical measures are mentioned in the DPA. Organizations are instead urged to take appropriate technical measures to prevent unauthorized access to or use of private data. Encryption should be one of those measures.	**General best practices for encryption would apply**: › Use of VPN technology for sending private data in transit › Use of whole-database or column-level encryption for any private data stored in databases › Use of full-disk or folder-level encryption stored on disk › Key management tools and procedures should be implemented for access controls to encrypted resources › Appropriate encryption policies should be in place

PERSONAL INFORMATION PROTECTION LAW (PIPL) OF 2003

FOCUS: Protection of the privacy of personal consumer data. Maintenance of adequate technical and administrative controls to protect stored data

SCOPE: Japan - All business and industries

PENALTIES: Fines, possible imprisonment up to 6 months

Requirements	Crypto Discussion	Best Practices
Article 20 of the Act states that any entity handling personal information must take necessary measures to prevent leakage, loss, or damage to that information.	No specific technical guidance is provided. Other administrative guidance is also mentioned. Encryption applies to protective measures necessary to protect leakage.	**General best practices for encryption would apply**: › Use of VPN technology for sending private data in transit › Use of whole-database or column-level encryption for any private data stored in databases › Use of full-disk or folder-level encryption stored on disk › Key management tools and procedures should be implemented for access controls to encrypted resources › Appropriate encryption policies should be in place

CALIFORNIA SENATE BILL 1386 (SB 1386)

FOCUS: General protection of individual's private information

SCOPE: U.S. - All organizations with customers and/or employees in the U.S. state of California

PENALTIES: Yes

Requirements	Crypto Discussion	SANS Best Practices
For organizations with customers and/or employees in the US state of California, the bill requires disclosure of a security breach where there is a reasonable belief that unauthorized access to unencrypted personal information has occurred. The bill specifically applies to data stored on computers. Any sensitive data not encrypted is subject to the disclosure provisions. A breach is defined as unauthorized access to or acquisition of computerized data that potentially compromises the security, confidentiality, or integrity of personal information.	Foundation legislation that has prompted similar legislation in other states (38 as of August, 2007). The U.S. Senate is currently considering a bill sponsored by Senators Leahy and Sanders called the Personal Data Security and Privacy Act of 2007 which would create a federal standard similar in nature to SB 1386.	**Encrypt the following data, at a minimum**: › Social security number › Driver's license number or California Identification Card number › Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account Any of the aforementioned data, when connected with an individual's first name or initial and last name, is considered to be sensitive personal data. **General best practices for encryption would apply**: › Use of VPN technology for sending private data in transit › Use of whole-database or column-level encryption for any private data stored in databases › Use of full-disk or folder-level encryption stored on disk › Key management tools and procedures should be implemented for access controls to encrypted resources › Appropriate encryption policies should be in place

Sources

1. http://www.sans.org/reading-room/analysts-program/encryption-Nov07
2. http://www.leg.state.nv.us/nrs/nrs-603a.html
3. http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
4. http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf
5. https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf
6. https://www.pcisecuritystandards.org/security_standards/glossary.php#S
7. http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security
8. https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ
9. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.html
10. http://www.out-law.com/articles/2012/october/ico-reiterates-warning-over-encryption-as-it-fines-council-120k-over-second-data-protection-breach/
11. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html
12. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.html
13. http://www.bbc.com/news/technology-25461353
14. http://www.esecurityplanet.com/network-security/insurance-company-fined-6.8-million-for-data-breach.html

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

1159-05.14DD.wpna.simple