


A background image showing a person's hand pointing at a laptop screen. Overlaid on the image are several semi-transparent circular gauges or dials with numerical markings, suggesting a technical or data-related context.

# Regulatory Compliance

A red dashed-line box containing the main title and subtitle.

## → Global Privacy, Disclosure and Encryption Issues

*A Trend Micro White Paper*

# REGULATORY COMPLIANCE

## GLOBAL PRIVACY, DISCLOSURE AND ENCRYPTION ISSUES

### I. INTRODUCTION

Information technology (IT) security is indispensable to an organization's ability to conduct business and achieve its objectives. With regulatory compliance and industry data security standards dominating many of these business objectives, confidential data protection comes to the forefront of IT security. Requirements vary among industries, geographies, and regions, but themes of privacy and breach disclosure recur across these regulations. And as regulators keep pace with business and technology, requirements become more specific—such as encryption of records to enforce confidentiality and avoid breach disclosure.

This paper provides an overview of the regulatory landscape and identifies steps to take for defining an effective compliance strategy.

### II. REGULATIONS CREATE WAVES WORLDWIDE

In simple terms, “compliance” is the adherence to an accepted policy or set of requirements. In the context of industry and regional regulations, compliance challenges organizations in proportion to the number of regulations that govern their business. Further complicating the compliance landscape are the various types of data that require protection.

#### ***CREDIT CARD DATA***

The Payment Card Industry Data Security Standard (PCI DSS) identifies specific controls over how credit card data is safeguarded, including where it is stored and where it is transmitted over public networks. PCI DSS is not a law on the books of a specific jurisdiction but it is quite effective nevertheless, since covered entities (such as merchants or payment processors) may be penalized by the payment card brand if they experience a breach or do not comply. To reinforce its importance, some jurisdictions have even codified these standards, as with the 2009 Nevada Senate Bill No. 227, which requires that ‘data collectors’ in that state comply with PCI DSS. This may be the beginning of a trend where local jurisdictions mandate compliance with this global standard. Not only does this trend further reinforce the importance of credit card security but it also opens the doors for civil penalties for related data breaches.

#### ***PERSONAL INFORMATION***

The European Union Data Protection Directive (EU DPD) mandates the adoption of standards for the collection, storage, and disclosure of personal data by member countries. For example, Section 47 of the EU DPD asserts that the email sender is in fact the ‘data controller’ for any personal data transmitted via email (§47 EU DPD). The UK Data Protection Act (DPA), taking guidance from the EU DPD, specifies that UK citizens are to be notified of how their “sensitive personal data” (such as religious and political beliefs) is being used and if it is part of a data breach. Switzerland, not part of the EU, also has the Swiss Federal Data Protection Act (DPA) and the Swiss Federal Data Protection Ordinance (DPO), which cover not only individual data but also legal entities.

In the U.S. alone, more than 700 state and federal privacy and surveillance laws were on the books in 2008 (Compilation of State and Federal Privacy Laws, Privacy Journal, 2008). Nevada mandates privacy of personally identifiable information (PII)—including names and credit card numbers—through encryption of

# REGULATORY COMPLIANCE

## GLOBAL PRIVACY, DISCLOSURE AND ENCRYPTION ISSUES

electronic communications (NRS 597.970), as well as breach notification (Section 359-C:19). Other state laws—such as Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00)—apply to all organizations that maintain personal information about a Massachusetts resident—whether they do business in the state or not. This regulation also requires encryption of all records transmitted across public networks as well as on all laptops or portable devices.

### ***CORPORATE FINANCIAL DATA***

Financial data privacy is partially covered by the aforementioned personal data protection requirements, but publicly held companies are also responsible for their own accounting practices. Fraudulent accounting practices in these companies brought about the 2002 Sarbanes Oxley Act (a.k.a. SOX) in the US, which requires separation of duties in the handling of financial information as a means to prevent fraud. SOX Section 404 includes auditing requirements for areas where there is a high risk of fraud—which for a financial accounting system could mean tampering of spreadsheets or unauthorized disclosure of company financials. Although many laud the Act with its reform of many corrupt accounting practices, critics charge that the guidelines are complicated and implementation is costly. Nevertheless, Japan soon followed suit with J-SOX but other regions such as Latin America and Asia Pacific countries such as Singapore and India have foregone enactment of laws in favor of implementing stronger audit practices in financial institutions.

### ***HEALTHCARE DATA***

In the US, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 provided a basis for the first federal standards designed to protect individual medical records. According to the U.S. Department of Health and Human Services (HHS) HIPAA Security Rule, healthcare providers are required to employ safeguards that “ensure the confidentiality, integrity, and availability of all electronic protected health information” under their control<sup>1</sup>. This data may include terms describing diagnosis, prescriptions, mental health, and payment status. The Health Information Technology for Economic and Clinical Health Act (HITECH Act) further reinforces the HIPAA rules with stricter breach disclosure requirements and extension of these rules to business associates of ‘covered entities’.<sup>2</sup>

## **III. RECURRING THEMES ACROSS REGULATIONS**

Although the number and complexity of industry mandates and regional laws can be overwhelming, there is a recurring theme of data protection. It all starts with confidential data, which is usually defined as an individual’s name, combined with other data such as credit card numbers, account numbers, health information, and financial data such as credit scores or bank information. Safeguarding the confidentiality of this data and taking responsibility for disclosing when this data is used or breached are key compliance drivers on a global scale. And as regulators keep pace with business and technology, requirements become more specific—such as encryption of confidential electronic records to enforce privacy.

# REGULATORY COMPLIANCE

## GLOBAL PRIVACY, DISCLOSURE AND ENCRYPTION ISSUES

Confidential Data Types	Description
PII: Personality Identifiable Information	Social security number/national identification number, drivers license number, address, phone number
PCI: Payment Card Industry	Credit card numbers, Card Verification Value (CVV), expiration date
PHI: Protected Health Information	Medical diagnosis codes, disease names, medication names, patient names
PFI: Personal Financial Information	Financial account number, credit score

Figure 1: Protected data types and data requirements

Confidential data is addressed differently depending on regional norms and industry best practices. Credit card data benefits from the global PCI DSS standard. Health (PHI) and personal data (PII) are covered by regional privacy laws, with additional focus in the US from the HIPAA and HITECH Acts. Financial data (PFI) is also often covered in these privacy laws but for matters of company financial data and the risks of data tampering, regions vary in their decision to enact laws (such as SOX in the US and J-SOX in Japan) versus exerting control through local auditing standards (such as CLERP 9 in Australia). The end result is a compliance landscape of frameworks, regulations, standards, and directives that ultimately impact businesses and government agencies that handle this data.

Geography	Confidential Data Addressed by Regional Laws			
	Privacy Regulations			
	PHI	PCI	PFI	PFI
Global				
North America				
U.S.	✓		✓	✓
Canada	✓		✓	✓
Europe				
E.U.	✓		✓	✓
U.K	✓		✓	✓
Switzerland	✓		✓	Covers best practices for validating controls
Germany	✓	✓	✓	—
Asia Pacific				
Japan	✓		✓	✓
Singapore	—		—	Covers best practices for validating controls
Australia	✓		✓	Covers best practices for validating controls
India	✓		✓	Covers best practices for validating controls
Latin America				
Brazil	Proposed		Proposed	Covers best practices for validating controls
Mexico	✓		✓	Covers best practices for validating controls

Figure 1: Common regulatory themes around the world

# REGULATORY COMPLIANCE

## GLOBAL PRIVACY, DISCLOSURE AND ENCRYPTION ISSUES

This simple overview confirms that governing bodies are well aware of risks to confidential data, but the degree and approach to which the laws mandate specific controls varies.

### ***PRIVACY DOMINATES THE COMPLIANCE LANDSCAPE***

While it is true that requirements vary across the global compliance landscape, all of these regulations ultimately aim to protect an individuals' privacy, usually by requiring that data associated with that individual is not visible to unauthorized users. Protecting individuals' personal, medical, and financial data is of utmost concern to enterprises not only for regulatory compliance but also for fear of brand damage, customer churn, and ultimately profitability. Governments share the same concerns, since citizens expect their government to safeguard their data as well.

Goals for achieving privacy have been made quite clear. Some requirements have been vague on implementation details such as the HIPAA Privacy and Security Rules, but subsequent guidelines (NIST 800-66) and laws (the HITECH Act) have stepped in to provide more implementation guidelines for enforcing privacy (of ePHI).

Although many nations and jurisdictions have had privacy laws on the books for decades, most were written for a paper-based world. But given recent initiatives for migration to electronic records, regulations have had to evolve to address electronic communications. As regulators keep pace with business and technology, more specific technical requirements are likely to materialize across industry and regional regulations.

### ***DISCLOSURE REQUIREMENTS***

Access to confidential data can be intentional or accidental. Either way, when personal data is involved, the regulators usually mandate that individuals be notified of how and when their confidential data is disclosed. The Swiss Federal Data Protection Act (DPA) regulates processing of personal data by entities in both private and public sectors—such that any time personal data is acquired, the subject must be notified. The UK Data Protection Act requires similar disclosure, and even mentions data collection via web-based forms.

But most data breach notification laws are designed to address data breaches as opposed to data access for legitimate use. These laws manage the risk of a breach that has already occurred, by notifying interested parties: the data subject, the regulating body, and in some cases the media. For example, the California SB 1386 law requires breach disclosure of data belonging to a “resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

The recent HITECH Act, which reinforces many of the HIPAA rules for safeguarding electronic Personal Health Information (ePHI), requires that the affected individuals, the media, and the Secretary of the Health and Human Services (HHS) department be notified if unsecured ePHI is breached. The notification must be timely and its content must include what happened and the type of unsecured PHI that was affected. Costs of these notifications are not trivial, with estimates at \$5.89 per affected user, according to the Interim Rules released subsequent to the Act. And the Act goes further to impose civil penalties on top of the breach disclosure requirements. Penalties for a confirmed breach (civil and monetary penalties effective February 18, 2010) are even worse, with a minimum of \$100 per affected user up to \$1.5 million total, within a calendar year.

# REGULATORY COMPLIANCE

## GLOBAL PRIVACY, DISCLOSURE AND ENCRYPTION ISSUES

### ***ENCRYPTION—DIRECT MANDATES AND EXEMPTION FROM DISCLOSURE REQUIREMENTS***

Perhaps the highly publicized data breaches of recent years were the catalyst, but regulators are increasingly calling out encryption as a specific technology required for securing confidential data. In some cases, encryption technology is also accepted as a compensating control for when data breaches cannot be prevented—allowing organizations to avoid costly breach disclosure requirements.

#### **Direct mandates**

PCI DSS was at the forefront of this trend, with requirements to encrypt credit card data where it is stored (PCI DSS Req. 3) and where it is transmitted (PCI DSS Req. 4). Since then, several US states have gone as far as to mandate specific technologies to enforce privacy, such as Nevada (NRS 597.970) and Massachusetts (201 CMR 17.00), which both mandate encryption of personal records transmitted over open networks. The Nevada law applies to business conducted in the state and goes further to require that data collectors in that state comply with PCI DSS as well. The Massachusetts law governs personal information of a resident of that state and specifies several other computer security requirements, including “reasonable monitoring of systems, for unauthorized use of or access to personal information”.

#### **Exemption**

Organizations can secure their confidential data and—in the case of the HITECH Act—avoid cumbersome and costly breach notification requirements with the use of encryption technology. The Act states encryption as the technology that can secure PHI, or render ePHI “unusable, unreadable, or indecipherable to unauthorized individuals such that breach notification is not required.” Such “breach notification exemptions” come into play for data at rest (i.e. storage) and data in motion (i.e. being sent out via email).

## **IV. IDENTIFY AN EFFECTIVE COMPLIANCE STRATEGY**

Even with similar data protection requirements, achieving compliance with all applicable regulations represents a significant undertaking. Enterprises must contend with large volumes and variety of business systems, gaps left by people and processes, and nuances between different data protection requirements. An effective compliance strategy must address these challenges in a manner that is efficient and scalable.

### ***EMPLOY A RISK-BASED APPROACH***

Compliance is about being effective in both implementing and auditing controls to meet compliance objectives. In the context of this discussion, these objectives include privacy, breach disclosure, and encryption.

In an ideal world, data protection would be applied to all networks and nodes where sensitive data *might* be transported, stored, or used. However, this level of protection is unrealistic due to operational limitations and budget constraints. Instead, the focus of IT operations should be on implementing security for systems that are high-risk, protect high-value data, or are most likely to present the greatest risk to the business if compromised. Similarly, IT audit teams routinely employ a risk-based approach to conducting audits to cover the most likely areas where confidential data is handled, as opposed to every system or user in the organization.

# REGULATORY COMPLIANCE

## GLOBAL PRIVACY, DISCLOSURE AND ENCRYPTION ISSUES

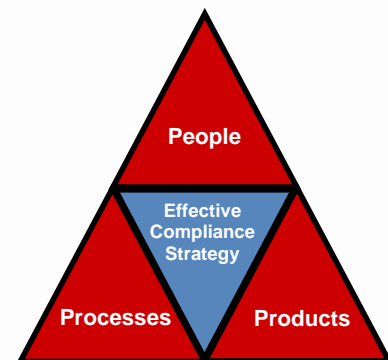
This approach is validated by international frameworks for IT such as CoBIT and specific data security standards such as PCI DSS. The latter mentions a risk-based approach to patch management (PCI DSS Req. 6.1), "...by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices..."

In practice, focusing on business systems where confidential data likely to be handled (such as email and end-user systems) and network storage locations (such as databases and file servers) is an effective approach.

### ***FOLLOW THE THREE P'S: PEOPLE, PROCESSES, PRODUCTS***

Achieving and maintaining compliance in an enterprise requires a combination of people, processes, and products.

Processes should be in place to secure confidential data throughout its lifecycle—creation, modification, storage, transmission, and destruction. People are largely responsible for following these processes, which is why compliance awareness training should be part of any compliance strategy.



In fact, many of the regulations themselves<sup>3</sup>—including PCI DSS, HIPAA, and FISMA—highlight awareness training as a compliance requirement. Some go even further to clarify people in the context of the confidential data. The UK Data Protection Act defines 'data subject' as the individual who is the subject of personal data and the 'data controller' as the one who would be responsible for this data—and therefore requiring compliance training.

While organizations will and should continue their compliance training efforts for each applicable regulation, they may also consider efficiencies in training by focusing on the common themes of privacy and breach disclosure requirements.

But people and processes are somewhat fallible. People make mistakes and unfortunately, in some cases commit fraud. Processes are only enforceable if they are documented. Yet most often in business environments, out of necessity, employees create ad-hoc processes to get things done rather than wait for actions to be documented. This is where products or "technology" become relevant.

Technology in particular is necessary to safeguard confidential data, which is increasingly available in electronic format and handled through enterprise systems such as such as email, databases, laptops, file servers, and more. Many enterprises are poised to see drastic increases in confidential data records due to recent regulations (with the HITECH Act of 2009) which reinforces the mandate for Electronic Medical/Health Records (EMR / EHR) by 2014.

More confidential data in electronic format means easier access to this data—as well as greater risk to its privacy and more likelihood of managing response to breach disclosure. Building on the risk-based

# REGULATORY COMPLIANCE

## GLOBAL PRIVACY, DISCLOSURE AND ENCRYPTION ISSUES

approach, products which safeguard confidential data over common protection points (email, end user systems and network storage systems) should be strongly considered to address privacy and breach disclosure requirements.

### **IMPLEMENT POLICY-BASED SOLUTIONS**

Review of global regulations uncovers the common themes of privacy and breach disclosure. Challenges for IT operations and IT audits suggest that securing high-volume, high-risk areas through automation with security technology is part of an effective compliance strategy. Identifying common compliance themes and protection points helps simplify the compliance challenge considerably. However, for most organizations, a single set of controls applied to users, data, and systems will simply not work. In contrast, policy-based solutions provide the ability to tailor IT security controls, a necessary capability since regulations vary in both scope and detail.

### **Safeguarding Confidential Data**

While one regulation may mandate encryption of this data, another regulation may require that sensitive data be monitored and protected, but may not specify how to do it. Where IT controls are not specified, organizations may interpret them differently as well. One organization may “monitor and block” confidential data from being emailed while another may decide to encrypt this content instead to allow privileged communications between authorized parties.

### **Controlling Privileged Access to Confidential Data**

At minimum, this requires policies that have end-user awareness through users’ network identities or email addresses. Japan’s Financial Instruments and Exchange Law (Japan FIEL) and U.S. Sarbanes-Oxley both require separation of duties and veracity in financial reporting, but Japan goes further to outline the IT security control environment, risk assessments, monitoring, and support. A policy-based data protection solution could address requirements for the Japanese branch of a multi-national company while also addressing less-prescriptive U.S. requirements.

Products must therefore support configurable policies to:

- Monitor different **data types** such as PII, PHI, PFI, and PCI
- Monitor different **user activity** such as email, web, instant messaging; copy/paste, printing, and copy files to USB/CD/DVD from end user applications. These channels or protection points often fall into three classes of data – or “data modalities”. They are Data in Motion (DIM), Data in Use (DIU), and Data at Rest (DAR)
- Monitor different **types of users** to determine their authorization to handle these data types
- Enforce different **controls**—such as audit, block, quarantine or encrypt



### V. ENABLING COMPLIANCE THROUGH DATA PROTECTION SOLUTIONS

Trend Micro™ Data Protection solutions help address regulatory compliance in the areas of privacy and breach protection. The solutions also provide encryption technology to address specific requirements to secure confidential data as it is transmitted over public networks or is stored within the corporate infrastructure.

#### ***DATA LOSS PREVENTION (DLP)***

The end-user system is often ground zero for data breaches. Employees—or insiders—routinely download, create, paste, or attach confidential data to their emails and send them to internal and external users. Some may copy this data to local peripheral storage devices (which leave the enterprise) and others may even share it with friends using peer-to-peer (P2P) software such as Skype. With all these scenarios to consider, keeping track of confidential data where it is used, transmitted, and stored is a considerable but necessary undertaking.

Both privacy and breach disclosure requirements benefit from the ability to discover, monitor, and prevent data breaches on end user systems. It is also necessary to conduct a regular inventory of where all this confidential data resides in the enterprise—be it end user systems or network storage systems. You have to know where your sensitive data is within your infrastructure in order to protect it. It is also essential to effectively respond to breach disclosure requirements and conduct breach investigations.

Trend Micro™ Data Loss Prevention (DLP) solutions address these challenges by monitoring and preventing information leaks across multiple threat vectors on end-user systems, including email, web, instant messaging, USB drives, and CD/DVDs. The software discovers confidential data on end user systems—whether online or offline—using highly accurate content matching and DataDNA™ fingerprinting technology. The solutions also help reinforce compliance awareness training with real-time messages that inform the user of their policy violation.

#### ***ENCRYPTION***

Ensuring that only authorized users view confidential data can mitigate risks associated with data breaches. Authorized accounts could be compromised, as in the case of lost or stolen laptops or the interception of confidential employee email communications.

Widespread use of laptops and remote access to enterprise data creates opportunity for data to be compromised by thieves and inadvertent loss of portable devices. Unencrypted data on laptops could be easily read from their hard drives. This is further complicated by email, which is not just a tool but also a business process. Both routine and privileged communications between employees and their colleagues, business partners, and customers rely on email services. Authorized employees access confidential data from the enterprise and are poised to share this information via email—either for legitimate business purposes or for unauthorized disclosure, be it accidental or intentional.

# REGULATORY COMPLIANCE

## GLOBAL PRIVACY, DISCLOSURE AND ENCRYPTION ISSUES

Encryption technology is therefore essential to prevent unauthorized visibility into data at rest, data in use, and data in motion.

Breach disclosure requirements in particular can be addressed by the ability to monitor and prevent data breaches over email. For some regulations, the requirements can be avoided all together (notification exemption) if it can be proved that the confidential data was “unusable, unreadable, or undecipherable” (as in the HITECH Act) when it was leaked or stolen. Privacy is directly enforced over email by encrypting confidential data. Policy-based, end-to-end, email encryption solutions enable organizations to address different privacy laws by automatically enforcing encryption of confidential data. For laws that require encryption of confidential data over open, public networks (such as PCI DSS, US state laws from NV, MA), email encryption directly addresses these requirements.

Trend Micro™ Encryption addresses privacy, breach notification and encryption requirements for email communications at key protection points—the end-user system and the email gateway. For policy-based encryption, which automatically detects confidential information at the email gateway and encrypts it without user intervention, Trend Micro offers email encryption for Trend Micro Hosted Email Security (an encryption service in the cloud) or Trend Micro Encryption for Email Gateway (on-premise encryption). Both of these solutions encrypt data between email gateways, but for employees who want to go further and secure communication from their end-user system to the email recipient, can leverage the Trend Micro Encryption for Email Client.

## VI. SUMMARY

The best approach to meeting any compliance requirement is to focus on highest risk, most-valued business systems (such as email and end user systems) and support a combination of trained people, documented processes and policy-based security solutions. For most enterprises contending with compliance across multiple regulations, this is likely to mean three things – (1) enforcing confidentiality of data (2) external notification in the event of a data breach (3) using encryption as a specific technology to address elements of the first two goals.

Trend Micro Data Protection solutions address all of these compliance concerns - privacy, breach disclosure, and encryption - with email encryption and Data Loss Prevention (DLP) solutions.

For more information, please visit [www.trendmicro.com](http://www.trendmicro.com).

# REGULATORY COMPLIANCE

## GLOBAL PRIVACY, DISCLOSURE AND ENCRYPTION ISSUES

### VII. EXHIBIT A

#### REGIONAL SAMPLING OF REGULATIONS, STANDARDS, FRAMEWORKS\*

##### Global

PCI DSS (Payment Card Industry Data Security Standard), ISO 19779/27001 (International Standards Organization) IT Security standard, ITIL (IT Infrastructure Library) framework for service delivery, COSO (Committee of Sponsoring Organizations) risk management in financial services, CoBIT (Control Objectives for Information and Related Technology) IT security standard

##### Americas

- **US:** HIPAA (Health Insurance Portability and Accountability Act), HITECH Act, SOX (Sarbanes-Oxley), GLBA (Graham Leach Bliley Act), FISMA, CA SB 1386, Nevada SB 227, Massachusetts 201 CMR 17.00
- **Canada:** PIPEDA, Bill 198 Multilateral Instrument

##### Europe

Euro-SOX, MiFID (Markets in Financial Instruments Directive), European Union Data Protection Directive 95/46, European Union Directive 2006/24/EC

- **UK:** Data Protection Act 1998
- **Germany:** German Federal Data Protection Act
- **Switzerland:** Swiss Federal Data Protection (DPA), Basel II, stricter audit procedures, (SCO) Swiss Code of Obligations

##### Asia-Pacific Japan

J-SOX, JPIPA (Japanese Personal Information Protection Act)

- **India:** stricter audit procedures
- **Australia:** Privacy Act, APRA (Australian Prudential Regulation Authority) Guidelines, CLERP 9

##### Latin America

- **Brazil:** Azaredo Law, Bill #6891/02
- **Mexico:** Ley del Mercado de Valores

\*Frameworks tend not to be mandatory but are used to develop best practices that can map to specific regulations.

##### Footnotes

<sup>1</sup> Department of Health and Human Services, "Health Insurance Reform: Security Standards; Final Rule." *Federal Register*, vol. 68, no. 34 (Feb. 20, 2003), pg. 8341. (<http://www.cms.hhs.gov/securitystandard/downloads/securityfinalrule.pdf>)

<sup>2</sup> Trend Micro Enterprise Security for the Healthcare Industry, "Assuring regulatory compliance, ePHI protection, and secure healthcare delivery."

<sup>3</sup> Security awareness training highlighted in PCI DSS v1.2 Req. 12.6, HIPAA Sec. 164.530(b)(1), FISMA AT-2