Regulatory Considerations for BYOD Policies

November 2012



The following white paper explores how current and future information security regulations could impact the way healthcare and financial institutions shape internal Bring Your Own Device (BYOD) policies.

HR HANOVER RESEARCH

Table of Contents

EXECUTIVE SUMMARY

The proliferation of mobile technology is transforming the workplace, with more and more companies allowing employees to bring their own smartphones, tablets, laptops, and other devices to work. In the hopes of transforming access into productivity gains, forward-looking chief information officers (CIOs) and IT departments are implementing corporate-wide bring-your-own-device (BYOD) policies to streamline and better manage the use of these devices.

One of the primary aims of BYOD policies is minimizing the risk of data being lost or compromised should a device go missing. Corporations in the highly-regulated industries of healthcare and finance face additional scrutiny and challenges. According to Littler Mendelson, a law firm focusing on employment and labor law solutions, the shift from IT policies that favored corporate-owned and distributed devices to employee-owned devices "clashes with the growth over the last decade of government regulations requiring companies to carefully protect the privacy and security of sensitive personal, financial, and health-related data."

Due to key legislation and regulations put in place in the United States, Canada, and the European Union (EU), there are often punitive implications for data breaches. To reduce risk and liability, companies in the healthcare and financial sectors must consider adding new layers of security to mitigate data loss and monitor information flow in case of an audit or investigation.

This report seeks to highlight the impact of specific regulations governing the healthcare and financial industries, along with potential security solutions offered by vendors of mobile device management (MDM) software. The following key findings provide a high-level perspective on requirements across the United States, Canada, and the EU.

- Governments in North America and Europe have placed responsibility on companies to closely monitor their financial and accounting activities and protect personal information from unauthorized access and prevent data loss. Businesses in both regions are **required to document risks and internal safeguards for protecting data from loss or compromise**.
- **Whereas Canada and the EU have adopted "omnibus" legislation on protecting personal data, the United States has put in place a patchwork of industry-focused laws and regulations**, including the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, and the Health Insurance Portability and Accountability Act.
- Broadly speaking, North American and European laws and regulations seek to protect consumers' sensitive data and increase the transparency of financial transactions. EU legislation, however, places more emphasis on the individual privacy of citizens. Therefore, **applying the "company property" concept to corporate data networks is less clear in the EU than in the United States**. This could further complicate the rollout of BYOD policies at a company-wide level.

- In the United States, healthcare and financial companies aim to verify internal controls and policy compliance on all mobile devices. While **strict enforcement and penalties apply to the healthcare sector, the financial sector has established largely voluntary compliance standards**/best practices to date.
- The introduction of **MDM platforms** as a part of BYOD policy provides a solution to many issues introduced by regulation: **control and security over corporate data, privacy and flexibility for employees to use their own devices, and a deeper layer of security measures to ensure compliance**.
- **MDM solutions** fill a technology gap and **help healthcare and financial companies effectively and efficiently introduce regulatory-compliant BYOD policies**. MDM providers typically employ a system of device encryption, remote wiping, firewalls, authentication mechanisms, access controls, and ongoing vulnerability assessments, among other practices, to meet both internal corporate and regulatory standards.

Legislation and Regulations

At the highest level, companies implementing BYOD policies must demonstrate their ability to meet and maintain all regulatory standards, but the policies and procedures used are largely developed on an organization-to-organization basis. In the United States, for example, evidence of ongoing risk assessments and internal monitoring are frequently-invoked requirements. The success of these assessments can bring about either non-intervention or damaging penalties.

Yet, many of these same regulations stop short of indicating which procedures or standards are sufficient to avoid punitive outcomes. Businesses, lacking guidance or transparency on how others develop internal benchmarks or risk mitigation standards, face a number of decisions on their own. Among the decisions made on a business level are: the kinds of information can and cannot be stored remotely or on cloud servers, how to verify the identity and access level of remote users, and how to retrieve data required for investigation or audit. The following chart provides a short overview of primary legislation affecting institutions and some of their specific implications for developing a BYOD policy.

Regulations and BYOD Policy Implications

Regulation/Legislation	Standards and Compliance Requirements	BYOD Policy Implications
Healthcare		
United States: Health Insurance Portability and Accountability Act (HIPAA, 1996)	▪ Encryption for patient health information, including electronic protected health information (ePHI) ▪ Policies and procedures that control the receipt and removal of electronic media that contain e-PHI in and out, as well as within, a facility ▪ Formal risk analysis processes	Concerns about access, storage, and the longevity of ePHI records on devices that can travel outside of protected areas necessitate strong oversight and advanced tracking capabilities for all employee-owned devices.
United States: Health Information Technology for Economic and Clinical Health Act (HITECH, 2009)	▪ Compliance with HIPPA requirements ▪ Demonstrably "active" policies to mitigate improper access to HIPAA data	Companies that are found to have experienced data breaches "due to willful neglect" are subject to seven-figure fines. Consequently, BYOD policies must demonstrate active efforts to meet HIPAA compliance and require employees to report lost or stolen devices.
Finance		
United States: Securities Exchange Act, Rule 17-A (1934/2003)	▪ Internal storage of all broker-dealer records in a digital storage medium or system that "preserve[s] the records exclusively in a non-rewritable, non-erasable format"	Rule 17-A could pose additional concerns around BYOD remote device wiping procedures, given the "non-rewritable and non-erasable" requirement.
United States: Sarbanes-Oxley Act (SOX, 2002)	▪ Retain all communications for seven years, including electronic communications ▪ Personal devices subject to review under investigations	Specifically, SOX requires that businesses verify internal controls on employee-owned devices, which could pose challenges to ensuring all

	▪ Companies must report annually on effectiveness of internal data security controls and policies	controls are maintained to the standards of the organization/not changed on individual devices.
United States: Gramm-Leach-Bliley Act (GLBA, 1999)	▪ Protect consumer information using a framework appropriate to each institution's "own circumstances" ▪ Implement information security programs that are required to include at a minimum: risk assessment, implementation and monitoring of safeguards, and system evaluation and adjustment ▪ Regular testing and monitoring of security systems	GLBA's lack of a unified or set procedure is particularly problematic for creating a BYOD policy. Financial institutions may not find comparable applications or enforcement contexts to use as a benchmark when developing their own policies. Similarly, they may have trouble defending why their systems are "adequate," so long as a risk of breach exists.
European Union: Data Retention Directive (2006/24/EC)	▪ Internal storage of extremely detailed telecommunications data for 6 to 24 months, which external government agencies are allowed to request access to ▪ Maintenance of a "fast and secure" retention system	Data on personal devices must be readily transferrable and available in its entirety to comply with access requirements.
Broad Consumer Protection and Right to Privacy Policies		
Canada: Personal Information Protection and Electronic Documents Act (PIPEDA, 2000)	▪ Implement retention policies for personal information ▪ Protect customer information from loss or unauthorized use ▪ Disclose data security policies	Organizations may spend a good deal of time updating and disseminating information on data security policies if BYOD policies are in flux.
European Union: Data Protection Directive (1995/46/EC)	▪ Provide safeguards for data adequacy, accuracy, and limited retention when personal data are collected ▪ Risk-appropriate protection of data processing, particularly the transmission of data over a network ▪ Issue notifications of personal data breaches	While the law specifies that businesses implement technical and organizational measures for data protection, including on employee-owned devices, it does not specifically "appropriate measures." It has been suggested, though not shown conclusively, that a minimum measure for BYOD policies would be enforcement of encryption standards.
United Kingdom: Data Protection Act (1998)	▪ Notification for individuals of any personal data collected, the purpose of data collection and processing, and any entities to whom the data may be disclosed	This personal data protection mandate extends to employees – according to the Data Protection Act, businesses must notify employees that they are monitoring personal data, including on employee-owned devices. This legislation was enacted to make the UK compliant with the EU Data Protection Directive.

UNITED STATES

There are three key pieces of legislation in the United States with implications for BYOD policies in the healthcare and financial sectors: the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act/Financial Services Modernization Act of 1999 (GLBA), and the Sarbanes-Oxley Act of 2002 (SOX).

Broadly speaking, relevant sections of HIPAA and GLBA focus on securing electronic data to protect consumers, while SOX places the responsibility on public companies to closely monitor their financial and accounting activities. The Health Information Technology for Economic and Clinical Health (HITECH) Act and the Securities Exchange Act also set forth requirements to ensure compliance in the healthcare and financial sectors, respectively.

HIPAA AND HITECH

HIPAA is the primary legislative framework guiding healthcare organizations in protecting the confidentiality, access, and integrity of ePHI. The legislation mandates that healthcare organizations ensure the confidentiality, integrity, and availability of patient health records.

HITECH, which took effect in 2009, was designed to encourage the use of information technology in the healthcare sector, while toughening measures to protect patient records and health information. HITECH imposes minimum penalties of $1.5 million for non-compliance of HIPAA, including penalizing violators who permit data breaches "due to willful neglect."

"U.S. Department of Health and Human Services upheld these fines after it concluded that these organizations either failed to take sufficient steps to encrypt patient data or neglected to properly develop a plan of action to mitigate data breaches."

Since October 2009, there have been 77 reported breaches of HIPAA and HITECH due to the loss and/or theft of mobile devices. Million-dollar fines have been levied against healthcare organizations in several cases. In 2010, Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates were fined $1.5 million in 2010 after the theft of an unencrypted laptop that held thousands of patient records. In 2012, BlueCross BlueShield of Tennessee was ordered to pay $1.5 million in violations after devices containing patient information were stolen. In June 2012, the Alaska Department of Health and Social Services received a $1.7 million fine following the theft of an unencrypted USB device that contained data of an undisclosed number of Medicaid recipients.

Often in such high-profile cases, the U.S. Department of Health and Human Services concluded that these organizations either failed to take sufficient steps to encrypt patient data or neglected to properly develop a plan of action to mitigate data breaches. Regulatory-compliant IT security procedures, especially those focused on **monitoring how data are stored or verifying the identity of the individual accessing the data, could have provided these organizations the tools to avoid the loss of sensitive information**.

GLBA, SOX, AND THE SECURITIES EXCHANGE ACT

GLBA requires financial institutions—defined as any company that offers consumers financial support or investment advice, loans, or insurance—to protect the sensitive personal and financial information of consumers. This includes names, addresses, debit and credit card numbers, credit histories, and Social Security numbers. In 2002, the U.S. Federal Trade Commission (FTC) issued the Safeguards Rule as a means to implement GLBA as a framework for developing, implementing, and maintaining the required safeguards, while leaving each financial institution the discretion to tailor information security programs to their "own circumstances."

The FTC recommends companies to develop "policies for [the] appropriate use and protection" of mobile devices in order to comply with the Safeguards Rule. This includes implementing information security programs, risk assessment, monitoring safeguards, and evaluation and adjustment of systems in place.

"In 2002, the Federal Trade Commission (FTC) issued the Safeguards Rule as a means to implement GLBA that "provides a framework for developing, implementing, and maintaining the required safeguards, but leaves each financial institution the discretion to tailor its information security program to its own circumstances."

While GLBA does not specify fines to be imposed upon violation, U.S. retailer T.J. Maxx agreed to settle a federal class action lawsuit for $6.5 million and with 41 state Attorneys General for $9.5 million after it failed to encrypt its electronic payments system over its wireless network, allowing hackers to steal an estimated 47.5 million credit and debit card numbers and other personal data. Similarly, in June 2012, an employee of a car dealership in the state of Georgia brought sensitive information home to work on his personal computer, where intrusive P2P software exposed and shared personal and financial information of 95,000 consumers. As a result, the FTC has filed a complaint against the dealership for violating the Safeguards Rule. The case has not yet been decided.

SOX aims at tightening corporate accountability, in part by requiring businesses to establish, maintain, and report adequate internal controls. Records of all communications, including those on employee-owned devices, must be stored for seven years if they could be tied to an audit or review. Rule 17a-4 of the Securities Exchange Act further requires all companies to preserve electronic records in a "non-rewriteable and non-erasable format," and provide immediate access to data in case of an investigation, for a period of seven years.

U.S. STATE REGULATIONS AND LEGISLATION

A myriad of state regulations and legislation further complicates BYOD policies and regulatory compliance in an environment where state laws co-exist with federal laws. Oregon requires businesses handling sensitive data to enact information security programs in writing and provide detailed requirements for implementation, while Texas imposes a general statutory duty on businesses to safeguard personal information. In Massachusetts,

information security regulations specify encryption requirements for personal information stored on mobile devices; financial penalties apply against businesses that fail to comply.

At least 29 states require the secure destruction or protection of personal information in electronic form. California state law requires notification of lost or stolen personal information, but recognizes that some organizations may not be required to disclose a breach if personal data is encrypted. Forty-five other states including Massachusetts, Illinois, Ohio and Texas, have enacted similar data breach laws to protect citizen privacy.

CANADA

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) obligates Canadian businesses to safeguard private data. PIPEDA requires businesses to protect customer information and disclose policies and practices regarding the collection of consumer information. While businesses are required to implement retention policies for personal information, the legislation requires companies to protect personal information from loss or unauthorized use, including electronic devices. PIPEDA created a legal mandate for businesses to protect sensitive private data through the use of encryption and firewalls.

In contrast to U.S. legislation, PIPEDA is focused more strongly on the goal to balance individual privacy protection (company data security policies) and the need of organizations to obtain such information for legitimate purposes. In addition, PIPEDA includes an international dimension, as it addresses cross-border data breaches and brings Canada's legislation in line with EU law that protects the personal information of EU citizens abroad.

EUROPEAN UNION

EU DATA PROTECTION AND DATA RETENTION DIRECTIVES

The EU Data Protection Directive (Directive 95/46/EC) addresses access and processing of personal data within EU member states. **While the United States prefers a sectoral approach to data protection legislation, the EU Data Protection Directive is an all-encompassing data protection law**, often described as an "omnibus" type of legislation that governs all written, electronic, and voice communications.

Similar to U.S. legislation, the EU Data Protection Directive requires risk-appropriate protection of data processing, particularly the transmission of data over electronic networks. Under the Directive, businesses are required to implement technical and organizational measures for data protection, including policies that cover employee-owned devices. While the law does not specifically outline specifics, companies must meet compliance by implementing standards, such as encryption.

Similar to Canada's PIPEDA, the Data Protection Directive focuses on personal privacy, and obliges companies to issue notifications of personal data breaches and permits personal data to be collected only for explicit and legitimate purposes and processed lawfully.

Further, the EU Data Directive implies that cloud-based email on an employee-owned device remains an employee's private property, regardless of whether those emails are for company business or not.

Thus, **the European approach differs greatly from data laws in the United States due to the focus on individual right to privacy**. The FTC has ruled that since an employer owns the network on which data and information (emails, internet access) is transferred, employees do not have any right to privacy. Moreover, information transmitted across an employer's network on an employee's device in the United States is considered "company property," while European law makes this question ambiguous.

The EU Data Retention Directive (Directive 2006/24/EC) requires public communications networks to retain data in a secure manner in case of law enforcement investigations. IT security entities are required to store telecommunications data for six to 24 months and ensure that their retention systems are fast and secure. Police and security agencies are able to request access to details such as IP address and time of use of every email, phone call and text message sent or received. The result is data retention regulations similar to those outlined in the United States SOX legislation, although it does not specifically focus on the financial sector.

EU Member States

EU member states are required to provide safeguards for data adequacy, accuracy, and limited retention. Germany's Federal Data Protection Act of 2002, harmonized with the EU Data Protection Directive, regulates the management of employees' personal data rather than applying to the protection of externally generated or stewarded consumer data. The law permits businesses to collect employees' personal data for certain purposes, irrespective of device ownership. To comply, businesses need to document collection of employee personal data, such as for employment and recruiting purposes.

The United Kingdom's Data Protection Act of 1998 oversees the protection of private employee information and requires that non-governmental data processors secure individuals' right to privacy. Businesses must notify employees that they are monitoring personal data, including on employee-owned devices. To make the United Kingdom compliant with the EU Data Protection Directive, the law requires that businesses notify individuals "in an intelligible form" of any personal data collected, the purpose of data collection and processing, and any entities to whom the data might be disclosed.

While France had a broad data protection law that predated the EU Data Directive, its Data Protection Act was harmonized with EU law in 2004. The law obliges organizations to appoint a representative to "take all useful precautions" to ensure that data is protected in compliance with the legislation and mandates that employees must consent to employers' processing of their personal data. Data is required data to be stored in a form that allows for easy retrieval, but no longer than necessary for the purposes required. French law requires

companies to keep an updated record of all personal data breaches and outlines fines and other sanctions for violations.

In Europe, **companies must appoint compliance representatives and describe how and why personal data will be processed**—but to varying degrees. German companies may be exempt from registering with the government if they appoint an internal data protection officer. The UK Data Protection Commissioner oversees compliance and enforces fines if companies neglect to register data notices. Meanwhile, France subjects companies to a series of data audits and approval before they can process any data.

VOLUNTARY AND SELF-REGULATED COMPLIANCE

Companies in the EU and North America do not solely rely upon government regulations regarding data protection. **Self-regulation and voluntary compliance bodies are a vital part of the broader regulatory framework, especially for the financial sector**.

"Self-regulation and voluntary compliance bodies are a vital part of the broader regulatory framework, especially for the financial sector."

A number of compliance mechanisms have been put in place by industry to support best practices in regards to protecting consumers, electronic data, and other sensitive personal information. Specifically relevant to BYOD policies, examples of voluntary/self-regulatory procedures include:

- **ISO 27001 and ISO 27002** are two IT security best practices providing legal, physical, and technical controls applicable to information risk management. These standards offer a risk-based approach and model for designing and implementing IT security systems. The ISO 27001/27002 framework emphasizes compliance as a key goal.
- **PCI DSS** is a financial industry standard initiated by the major electronic payment system companies to harmonize security protocols they impose on merchants, payment service providers and banks. PCI DSS applies to any organization that has a merchant ID and either transmits or processes data related to credit card holders and establishes requirements for encryption, authentication, and auditing.

SOFTWARE SOLUTIONS

While security drives the growth of this technology, mobile device management (MDM) solutions offer companies in the healthcare and financial industries the opportunity to comply with a host of North American and European laws and regulations. An effective MDM platform can ensure regulatory compliance when implementing the transition toward a corporate BYOD regime, as well as help IT departments better manage their data security.

A May 2012 survey of MDM vendors conducted by technology research firm Gartner concludes that MDM is "the fastest-growing enterprise mobile software ever, in terms of number of suppliers, revenue growth and interest from clients." The survey included products that provide password enforcement, remote data wiping and device locking, automatic audit trail creation and tracking of device logins, jailbreak detection, and support for anti-virus software, encryption, firewalls, and mobile virtual private networks (VPNs).

Software can only mitigate, not eliminate, security risks. The introduction of MDM systems into a company's BYOD policy provides a solution to addressing key regulatory issues:

1) Corporate control and security over sensitive data,
2) Privacy and flexibility for employees to use their own devices, and,
3) A deeper layer of security measures to ensure regulatory compliance.

The legislation and regulations outlined above hold considerable implications for the implementation of BYOD policies. The web of sector-based and international laws create an added layer of complexity for IT decision-makers. Data protection regulations and penalties for the U.S. healthcare industry are clearly outlined in HIPAA and HITECH, whereas companies in the financial sector must take measures to prevent information loss on missing devices while ensuring that all data is accessible case of an investigation. The rise of mobile devices has also accelerated the lifecycle of privacy laws. While corporate BYOD policies may meet regulatory compliance today, ad hoc updates and changing concepts of right to privacy may significantly alter applicable regulations in the coming years.

> *"Gartner concludes that MDM is the fastest-growing enterprise mobile software ever, in terms of number of suppliers, revenue growth and interest from clients."*

HEALTHCARE COMPLIANCE

The introduction of employee-owned devices raises concerns about access, storage, and the longevity of ePHI records on devices that can travel outside of protected areas within healthcare facilities. When introduced into healthcare institutions' BYOD policies, MDM features can expand the way mobile technologies are used, while mitigating the threat of patient data loss and supporting compliance with regulatory mandates. Best practices for ensuring compliant mobile technologies include:

- Store ePHI data only on password- protected and encrypted mobile devices
- Install backup, restore, and remote wipe features on lost or stolen devices containing ePHI
- Use secure VPN or SSL when connecting to transmit ePHI over the internet and enable password protocols/advanced identification technologies before permitting network access
- Link MDM systems with network access control to provide additional layer of security
- Limit/monitor third-party applications installation on corporate-owned devices and additional password protocols for company-owned applications
- Enact security and compliance management policies, procedures, and reporting facilities to ensure maintenance of employee compliance and permit evidence to authorities in case of an audit
- Block network access for devices not including MDM software and report any devices attempting to access system without MDM software

FINANCIAL SECTOR COMPLIANCE

The dual requirements of data retention and prevention of data compromise represent the largest challenges for financial sector companies moving toward BYOD policies, as financial institutions and other business with customer financial information on record are frequently the victims of sophisticated attacks on their security systems. Security threats exposed by improper controls over personal mobile devices have caught the attention of regulators and companies who need to protect consumer and investor data. Nevertheless, a lack of defined regulatory standards makes it difficult to anticipate how rules will be applied or in which direction they may develop. MDM solutions can help companies meet compliance through the following technology solutions:

- Remote wipe capabilities to mitigate risk of exposing financial information
- Unified control of both applications (e.g. customer relationship management software) and MDM platforms to ensure data retention and reporting requirements
- Integration between devices and servers allowing email to be captured and retained according to company policy and regulatory guidelines and the retention of data through remote servers that is immediately accessible in case of an audit
- Control over which devices are permitted to access a corporate network to prevent leakage of sensitive data as a result of lost or stolen mobile devices
- Demonstrate active, voluntary compliance with industry best practices (e.g. PCI DSS) through the implementation of encryption and auditing

RIGHT TO PRIVACY

The drive to manage the mobile devices can, by the same turn, raise concerns over employees' right to privacy. This is particularly challenging for U.S.-based or other multi-

national companies which face changes in the definition and reach of "company property" from country-to-country. In effect, it may change both the nature of what a BYOD policy can specify and how it can be rolled out evenly across the organization. MDM software offers several solutions to meet these compliance issues for multi-national companies:

- Software consoles to enforce security protocols: passwords, access to applications, encryption, remote lock-down, and regulatory compliance management
- Encryption of customer information via mobile devices and company networks to fulfill consumer protection benchmarks
- Ability to distribute company BYOD policy manuals—including privacy notifications—from a central server, and report which employees have read the mandates
- Time-based controls that grant employees access to customer data only during business hours
- Privacy features that restrict administrators from seeing non-corporate or personal applications installed, or that deactivate devices' IP addresses and geographical coordinates

Project Evaluation Form

Hanover Research is committed to providing a work product that meets or exceeds member expectations. In keeping with that goal, we would like to hear your opinions regarding our reports. Feedback is critically important and serves as the strongest mechanism by which we tailor our research to your organization. When you have had a chance to evaluate this report, please take a moment to fill out the following questionnaire.

http://www.hanoverresearch.com/evaluation/index.php

Caveat

The publisher and authors have used their best efforts in preparing this brief. The publisher and authors make no representations or warranties with respect to the accuracy or completeness of the contents of this brief and specifically disclaim any implied warranties of fitness for a particular purpose. There are no warranties which extend beyond the descriptions contained in this paragraph. No warranty may be created or extended by representatives of Hanover Research or its marketing materials. The accuracy and completeness of the information provided herein and the opinions stated herein are not guaranteed or warranted to produce any particular results, and the advice and strategies contained herein may not be suitable for every member. Neither the publisher nor the authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Moreover, Hanover Research is not engaged in rendering legal, accounting, or other professional services. Members requiring such services are advised to consult an appropriate professional.

1750 H Street NW, 2nd Floor
Washington, DC 20006

P 202.756.2971 F 866.808.6585
www.hanoverresearch.com