

Increasingly On the Go: Mobility Compliance in Regulated Industries

How financial institutions, healthcare companies, government agencies, and other regulated entities maintain successful—and compliant—mobile deployments.

**Your
Device
Here.**

Good supports
hundreds of devices.



A small red square is located to the left of the 'Contents' header.

Contents

- Executive Summary 3**
- Mobile Devices Become Work Devices 3**
- Regulatory Compliance Challenges 4**
- Key Strategies 6**
- Good Solution 7**
- Conclusion 9**

Executive Summary

As mobile devices increasingly become popular work devices, enterprises and government agencies must weigh the benefits of greater employee productivity against potential security risks. In addition, companies in highly regulated industries face the ever-present challenge of meeting regulatory requirements.

This document discusses mobility trends, key regulations as they apply to mobile devices, and strategies that enterprises and government agencies can pursue to address security and compliance.

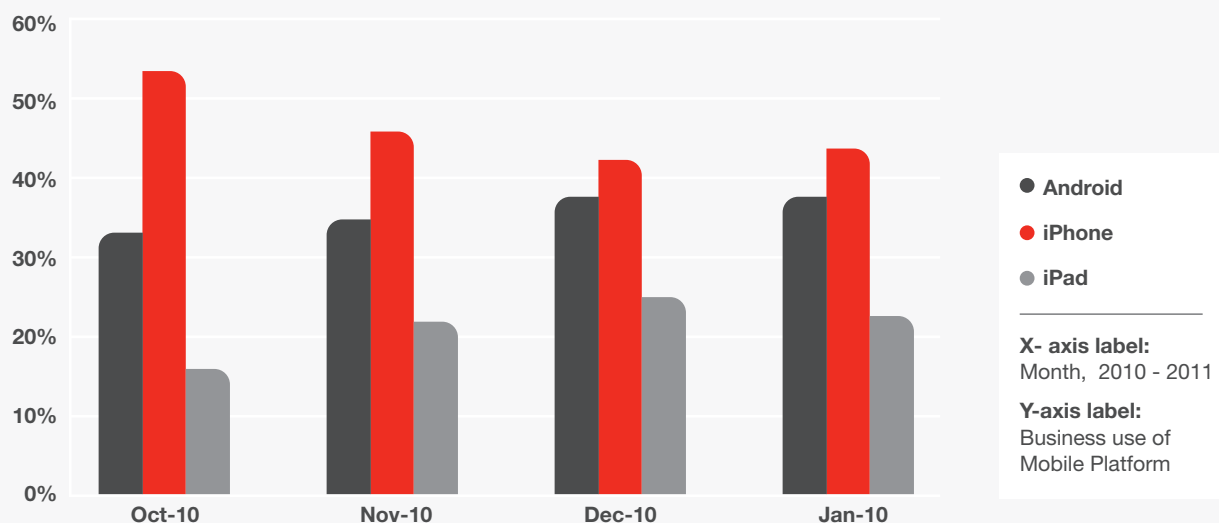
Mobile Devices Become Work Devices

Mobility in the enterprise and government is undergoing a dramatic shift. In particular, Forrester Research predicts that “As smart phones continue to develop, it will become possible to use them as primary work devices.”

Examples of the growing use of mobile devices in work-related activities include:

- Investment brokers sending emails from their smart devices, notifying customers about new investment opportunities
- Doctors using tablets as the new “computer on wheels” to access patient information
- Insurance agents using their devices to connect to the company network and obtain the status of customers’ existing life insurance policies
- Public health care workers using mobile devices to access and update case information
- Public officials using their devices to negotiate contracts and budgets

Based on a survey of thousands of enterprise companies and government agencies by Good Technology, more employees are choosing to use their own personal mobile devices for work. Often these are non-Blackberry devices, including iOS and Android devices. Apple’s iOS devices—which represent more than 65% of net new activations from October 1st through December 31st 2010—are currently the preferred non-Blackberry devices used within enterprise and government organizations. At the same time, Android device and tablet activations continue to show strong growth.



In addition to monitoring the growth of iPhones and Android devices in the enterprise, similar research by Good Technology revealed a dramatic increase in the use of iPads in business, which jumped from 0% to 22% of overall activations by the end of 2010.

Regulatory Compliance Challenges

Although the increased use of mobile devices as work devices can result in higher levels of productivity, many organizations are concerned with the possible security risks—especially those organizations in highly regulated industries, such as healthcare, financial services, and government.

The following is a quick review of key regulations and implications related to protecting confidential information on mobile devices.

HITECH

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act took effect. HITECH was developed to further encourage the use of health information technology to save lives and reduce costs. HITECH requires that healthcare organizations take more responsibility for protecting patient records and health information, and requires greater accountability for covered entities to comply with HIPAA. Non-compliance can incur penalties as high as \$1.5 million dollars for data breach.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 established guidelines for healthcare organizations to standardize the manner in which personal health information is electronically handled and protected. The HIPAA Security Rule provides guidelines and implementation specifications for how healthcare organizations should protect the confidentiality, integrity, and availability of electronic-protected health information (ePHI).

In 2006, in response to the increase of mobile devices in the industry, the Center for Medicare and Medicaid Services (CMS) released new HIPAA guidelines to protect mobile devices. In addition, CMS published a document entitled “HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information,” which provides guidance to healthcare entities regarding the protection of electronic protected health information (ePHI). [<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remotese.pdf>].

The HIPAA Security Guidance template below is a useful tool for healthcare organizations when considering security controls related to protecting ePHI on mobile devices:

HIPAA Criteria	Questions
Workforce Security	Is all Electronic Protected Health Information (ePHI) that is stored on a mobile device password-protected and encrypted?
Security Incident	Are employees required to report lost or stolen devices?
Contingency Plan	Are Backup and Restore procedures in place in the event a device is lost or stolen?
Access Control	Do you limit employee access from a mobile to a company network based on your security policies? Do you verify that the device meets your security requirements (e.g., device make, operating system version) before allowing network access?
Device Control	If a device is lost or stolen, do you perform a remote wipe to erase ePHI? Do you prevent third-party applications from being installed on corporate-owned devices in accordance with your security policies?
Authentication	Does your authentication management program provide a strong password protocol for accessing the device, corporate data, and applications?
Integrity	Do you have security and compliance management policies, procedures, and reporting facilities in place to ensure maintenance of employee compliance—while also providing evidence to auditors?
Transmission Security	Do mobile devices use secure VPN or SSL when connecting to transmit ePHI over the Internet?

US-SEC Rule 17a-4/NASD 3010/3110

With widespread use of electronic communications on mobile devices for business purposes, many financial services organizations are implementing necessary mobile security policies to protect investor information and comply with regulations such as U.S. SEC-17a-4, NASD 3010, and NASD 3110. These regulatory guidelines generally require covered entities to retain and protect the integrity of communications—including electronic communications—with investors.

Examples of compliance include financial services companies encrypting, capturing, and storing email messages sent to and received by mobile devices. Other organizations are implementing remote wipe and device lockout of lost or stolen mobile devices to prevent data loss of investor information.

On a related note, the Financial Services Authority (FSA), the independent regulating body for financial services institutions in the U.K., is requiring that by November 2011, financial services organizations record traders' mobile voice conversations related to client orders and to archive these conversations for six months. The ruling is another example of regulators' concern with the increase in mobile device adoption for business purposes, and the related security risks.

GLBA and Safeguards Rule

The Gramm-Leach-Bliley Act or GLBA requires that financial institutions protect consumers' personal information such as their names, addresses, phone numbers, bank and credit card numbers, income and credit histories, and social security numbers. The Federal Trade Commission issued the Safeguards Rule as a means to implement the GLB Act. The Safeguards Rule requires financial institutions to keep customer financial information secure, including information on mobile devices. The FTC offers several recommendations for institutions including the development of "policies for the appropriate use and protection" of cell phones or other mobile devices. The FTC also recommends that institutions encrypt consumer information.

FISMA

The Federal Information Security Management Act of 2002 or FISMA requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Subsequent to the passing of FISMA, the National Institute of Standards and Technology (NIST) released guidelines on security controls for Federal Information Systems via special publication 800-53. The risk management framework in NIST 800-53, Revision 3, provides civilian federal agencies with guidelines for breaking down FISMA into areas of IT control that can be implemented as policy, and assessed for compliance to all components of an information system that processes, stores, or transmits federal information.

California SB 1386

California SB 1386 was one of the first state laws requiring the notification of lost or stolen personal information. What's interesting to note is that California SB 1386 as well as other similar breach notification laws recognize the benefits of encrypted data. As such, in some cases organizations may find that they will not be required to disclose a breach if personal data, including data on a mobile device, is encrypted. In addition to California, 45 other states including Massachusetts, Illinois, Ohio and Texas, have enacted similar data breach laws to protect citizen privacy.

Key Strategies

Embrace Choice

Rather than prohibit employees from using the mobile devices of their choice due to security or regulatory concerns, organizations should do just the opposite, and embrace employee choice. As noted by Gartner Analyst Nick Jones, "Internal corporate policies should focus on regulating behavior rather than devices...."

In addition, compliance should enhance mobility, not restrict it.

Employees allowed to use personal devices are more productive and responsive to clients and constituents. In addition, these employees are more willing to access enterprise and agency data in a managed and secure way, rather than by circumventing company or agency security controls.

Finally, by allowing employees to choose their own mobile devices, companies will be able to attract greater talent.

Protect Confidential Information

Securing a mobile device has unique challenges compared to protecting an employee's desktop. For example:

- Due to their form factor, mobile devices are more easily lost or stolen.
- An attacker can hijack a smartphone's Bluetooth connection and use it to access company network resources.
- The risk of potential corporate or agency data loss is significant with the growth of and easy access to mobile applications. Many of the most popular business applications include the ability to save data and files in unprotected locations.
- Companies faced with having to manage different mobile devices need to implement multiple security policies based on each manufacturer's model and operating system.
- For individual-liable devices, if the device is lost, a remote wipe may require removing personal information, along with company information.

However, by following security best practices and using automation as much as possible, IT organizations can reduce the risk of security threats and related IT costs. Key security strategies include:

- Developing, managing, and enforcing consistent mobile security policies
- Strong authentication and access control
- Data encryption
- Implementing security at the application level to prevent mobile data loss
- Device lock and wipe
- Data retention for audit and forensics.

Good Solution

The Good for Enterprise (GFE) mobile solution provides secure end-to-end, wireless, real-time messaging, collaboration, and Intranet access supported by comprehensive device management. GFE helps regulated companies protect their mobile devices from security threats and meet compliance requirements.

Good Security Approach

Good for Enterprise provides end-to-end security, protecting confidential information on the mobile device, over-the-air (OTA), and on Good servers. In addition, Good's security approach provides the flexibility to manage both personally-owned and corporate-owned devices from a single solution. For personally-owned device, Good's secure container enables IT organizations to implement policies at an application level, protecting only company information while leaving personal data intact. For corporate-issued devices, IT can secure the entire device, locking down device features such as camera and browser via mobile device management polices.

Good Security Controls

Good for Enterprise offers a comprehensive set of security controls to help companies meet regulatory compliance, including:

- AES 192-bit encryption of data on the device and over-the-air, including email, attachments and contacts
- Strong password protection
- Two-factor authentication
- Secure browser
- Rooted Device / Jailbroken device protection
- Remote wipe/lock of only corporate data or the entire device
- No inbound firewall holes
- Emergency access
- Time-based lockout
- Definition of allowed device type
- Role-based administration
- Prevention of cut, copy, and paste
- Warnings to minimize emails to restricted parties
- Prevention of sending SMS messages from the Good app
- Verification of device connectivity and remediation if device does not connect in specified timeframe
- Prevention of access to camera, AppStore, Safari browser, and more



Good's security container separates company and personal information.

Managing Compliance

Good for Enterprise portal and server logs allow administrators to monitor and enforce mobile device compliance with company security policies, and also help IT demonstrate compliance to internal and external auditors.

In order to address data retention requirements by some regulations, Good for Enterprise allows companies to capture email communications, contact, and calendar data through integration with Domino and Exchange servers.

Finally, with Good for Enterprise's broad platform support, IT can easily manage compliance across a fleet of heterogeneous devices. This is especially critical given that security capabilities vary based on the make and model of each device and operating system.



The following table outlines how Good for Enterprise addresses key regulations.

REGULATION	GOOD CAPABILITIES
NYSE & NASD SEC 17-A “Joint Guidance” require brokerage firms to capture broker/dealer communications with customers.	Good for Enterprise integrates with your company’s email servers, allowing broker/dealer email to be captured and retained according to company policy and regulatory guidelines.
Gramm-Leach-Bliley Act (GLBA) requires that financial institutions protect information collected about individuals, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers.	Good’s Personal Information Management ensures that customer contact information is encrypted on the mobile device, OTA, and on Good servers.
Health Insurance Portability Act (HIPAA) requires that email communication related to patient health information be encrypted.	Good for Enterprise uses AES 192-bit, FIPS-certified encryption to encrypt data on several layers, including email messages on the mobile device, OTA, and on Good servers.
The American Recovery and Reinvestment Act (ARRA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), prohibit the storage of unencrypted personally identifiable information (PII) and protected health information (PHI) on computing devices, including smart phones.	Good’s Secure Enterprise Container encrypts documents containing customer information on mobile devices.
California SB1386, Massachusetts 201 CMR 17, and a number of other state data breach laws require the notification of lost or stolen personally identifiable information such as social security number or drivers license number, unless the data is encrypted. If the data is encrypted, organizations may not need to disclose the breach of personally identifiable information.	Good for Enterprise uses AES 192-bit, FIPS certified encryption to protect data transmitted over the air and at rest on the device. Good also provides a number security capabilities such as password requirements, remote wipe and mobile data loss prevention policies that can reduce the risk of data breach.

Conclusion

With the right set of policies, procedures, and technologies—such as Good for Enterprise—companies can embrace employee use of mobile devices, whether company-owned or individually-owned, while still meeting security and regulatory requirements.

To learn more about Good solutions, call **866-7-BE-GOOD** or visit **www.good.com**.



Good Technology
For more information,
please call 866 7 BE GOOD
or visit www.good.com.

Global Headquarters
+1 408 212 7500 (main)
+1 866 7 BE GOOD (sales)

EMEA Headquarters
+44 (0) 20 7845 5300

Asia/Pacific Headquarters
+61 (02) 92381953

©2011-2012 VISTO Corporation and Good Technology, Inc. All rights reserved. Good, Good Technology, the Good logo, Good for Enterprise, Good for Government, Good for You, Good Mobile Messaging, Good Mobile Intranet, and Powered by Good are trademarks of Good Technology, Inc. ConstantSync, Constant Synchronization, Good Mobile Client, Good Mobile Portal, Good Mobile Exchange Access, Good Mobile Platform, Good Easy Setup, Good Social Networking and Good Smarticon are either trademarks or registered trademarks of VISTO Corporation. All third-party trademarks, trade names, or service marks may be claimed as the property of their respective owners. Good and Visto technology are protected by U.S. patents and various other foreign patents. Other patents pending.

WP_MobileCompl_Nov2011_US