

BlackBerry and Health Insurance Portability and Accountability Act (HIPAA) Guidelines

Author: J. Tikkanen, JJT Consulting Group

Sponsored By: Research In Motion

Forward

About this White Paper

This white paper is sponsored by Research In Motion® (RIM®) and written by JJT Consulting Group with editorial input from RIM.

About the Author

JJT Consulting Group is a high-technology focussed consultancy providing research and advisory services to companies operating in the communications and healthcare sectors. Its principle, Jack Tikkanen holds an MBA and has over ten years of experience working with a variety of sector companies in technology research, marketing and strategic development. JJT Consulting Group holds a third-party relationship with Research In Motion (RIM) and was contracted to research and develop a white paper evaluating RIM's BlackBerry® solution in terms of the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Table of Contents

Executive Summary.....	1
Section 1: The Health Insurance Portability and Accountability Act (HIPAA)	1
What is HIPAA?.....	1
Privacy Rule Compared to Security Rule.....	1
Who is Affected?	2
HIPAA Compliance Deadlines	2
What are the Penalties for Non-compliance?	2
HIPAA Requirements	2
Protected Health Information (PHI)	2
The Privacy Rule.....	3
The Security Rule.....	3
Section 2: Mobile Devices in Healthcare.....	5
Growing Use of Wireless Devices.....	5
The BlackBerry Enterprise Solution in Healthcare.....	6
Section 3: Best Practices for Wireless Device Management	7
Common Wireless Threats and Vulnerabilities	7
Authentication Methodologies	7
Mitigating Wireless Vulnerabilities.....	9
BlackBerry and HIPAA Technical Safeguards Best Practices.....	11
Conclusion	12
BlackBerry Enterprise Server Architecture.....	13
Encryption and Authenticity.....	14
End-to-end Wireless Encryption.....	14
BlackBerry Enterprise Server Permits Only Trusted Connections.....	14
HTTPS for Secure Data Access.....	14
S/MIME Support	14
Strong IT Policy Enforcement and Management for BlackBerry Devices.....	15
Certified Secure.....	15
Independently Audited Security Model.....	15
Java-based BlackBerry Devices	15
Bluetooth Support on BlackBerry Handhelds.....	15
Deleting Device Data.....	16
Password Keeper	16
Attachments	16
Focus on Corporate Features for Added Security	16
IT Policies for Security Settings	17
Sources.....	17
Resources.....	18
End Notes	18

Executive Summary

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a broad and comprehensive set of regulations requiring healthcare organizations to address privacy and security concerns related to electronically stored and transmitted healthcare data. HIPAA's Security Rule mandates technical safeguards and further details the security standards to be implemented by organizations for the protection of electronic data. Although the Security Rule provides covered entities with implementation specifications describing how the standards are to be implemented, HIPAA is designed to be technology-neutral. Individual organizations must make the decision on which technology solutions allow the organization to comply with HIPAA requirements. Accordingly, wireless devices are not specifically detailed in HIPAA's Security Rule but must be viewed in the context of the healthcare organization's entire system for electronically storing and transmitting data.

The Security Rule applies to the integrity and security of an entire IT system, encompassing front-end devices such as the BlackBerry device, and including back-end processes and servers such as the BlackBerry Enterprise Server™. The technical safeguards specified in the Security Rule can be regarded as IT security policies standard to any fully protected system (i.e., unique user identification, data encryption) and can be viewed as an archetype for how an organization can safeguard its data. Therefore, wireless solutions should be evaluated on the basis of how the solution's available security features and functionality enable the organization to meet the technical safeguard specifications described in HIPAA's Security Rule. The BlackBerry solution provides strong end-to-end security features and functionality from the BlackBerry device to the BlackBerry Enterprise Server, such as Triple-DES or AES encryption of all transmitted data, which meet HIPAA specifications. No formal certification process is included in HIPAA, however BlackBerry possesses security features and capabilities enabling it to operate fully within a HIPAA compliant environment.

Section 1: The Health Insurance Portability and Accountability Act (HIPAA)

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted by the Department of Health and Human Services (HHS) for two key reasons:

1. To protect the confidentiality and security of individual patient health data by setting and enforcing standards; and
2. To improve the efficiency of healthcare delivery through the standardization of electronic data interchange.

HIPAA established the "Privacy Rule" and the "Security Rule" for the handling and security of medical records. The Privacy Rule governs the use and disclosure of Protected Health Information (PHI) in any form (electronic, oral, and/or paper), while the Security Rule is concerned with the security standards for PHI in electronic format (E PHI). The Security Rule is applicable to the security of data stored and exchanged through mobile wireless devices such as BlackBerry.

Privacy Rule Compared to Security Rule

The Privacy Rule requires covered entities to develop appropriate administrative, physical, and technical safeguards for PHI and to reasonably implement those safeguards. The Security Rule focuses exclusively on protecting the confidentiality, integrity and availability of E PHI. The key distinctions between the Privacy Rule and Security Rule are:

1. Electronic vs. paper and oral: the Privacy Rule applies to all forms of PHI (electronic, written, and oral). The Security Rule applies only to E PHI, encompassing E PHI that is created, received, maintained or transmitted.

2. Privacy Rule "Safeguard" requirement: the Privacy Rule contains several provisions requiring covered entities to implement safeguards for PHI. In contrast, the Security Rule provides specific security requirements at a more granular level of detail than that provided for by the Privacy Rule.

Who is Affected?

Any healthcare organization (HCO) storing health information electronically or using electronic transactions for the exchange of health information must achieve HIPAA compliance. In general, the following are considered to be covered entities:

1. Covered Health Care Providers: Any provider of medical or other health services or supplies transmitting any health information in electronic form in connection with a transaction for which HHS has adopted a standard.
2. Health Plans: Any individual or group plan providing or paying for the cost of medical care.
3. Health Care Clearinghouses: Public or private entities processing another entity's health care transactions from a standard format to a non-standard format, or vice-versa.
4. Medicare Prescription Drug Card Sponsors: A nongovernmental entity offering an endorsed discount drug program under the Medicare Modernization Act.

HIPAA compliance is a top priority for healthcare Information Technology (IT) executives. The *16th Annual HIMSS Leadership Survey sponsored by Superior Consultant Company/ACS Healthcare Solutions*ⁱ found that forty-four percent of IT executives identified upgrades of IT security systems to HIPAA requirements as a top priority in 2005. Thirty-five percent of healthcare IT executives surveyed viewed compliance with HIPAA's security regulations as a top priority for 2005.

HIPAA Compliance Deadlines

The Privacy Rule became effective on April 14, 2001, with full compliance of the Privacy Rule required by covered entities as of April 14, 2003 except small health plans which had until April 14, 2004. The Security Rule, published April 21, 2003, specifies that compliance must be achieved by most covered entities as of April 21, 2005, except for small health plans which have until April 21, 2006.

What are the Penalties for Non-compliance?

HIPAA standards and proposed rules call for severe civil and criminal penalties for non-compliance. Penalties include fines of up to \$25K for multiple violations of the same standard in a calendar year; and fines up to \$250K and/or imprisonment up to 10 years for wilful misuse of individually identifiable health information. The Office for Civil Rights (OCR) within HHS oversees and enforces the Privacy Rule, while the Centers for Medicare and Medicaid Services (CMS) oversees and enforces the Security Rule.

HIPAA Requirements

Protected Health Information (PHI)

PHI consists of all individually identifiable health information. This refers to information that either identifies an individual or provides a reasonable basis by which the information can be used to identify an individual. PHI includes information explicitly linked to an individual such as medical records, name and social security number, and also includes health information that could reasonably be expected to identify an individual such as an e-mail address or telephone number. PHI is transmitted in many forms and mediums, including oral, paper, and electronic, by many organizations including employers, health care providers, health plans, and health care clearinghouses.ⁱⁱ

The Privacy Rule

The Privacy Rule establishes standards for how covered entities should control protected health information (PHI) that is "transmitted or maintained in any form or medium" including paper records, faxes and oral communications. The rule is intended to protect the privacy of all individually identifiable health information, regardless of whether the information is or has been in electronic form.

The Security Rule

The Security Rule focuses on safeguarding the confidentiality, integrity, and availability of all EPHI that a covered entity creates, receives, maintains, or transmits. The Security Rule details essential standards and describes addressable and required implementation specifications. The rule stipulates that covered entities must protect EPHI against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures, and must ensure compliance by their workforce. Required safeguards include implementing appropriate policies and procedures, safeguarding physical access to EPHI, and ensuring that technical security measures are in place to protect networks, computers and electronic devices.

Section 164.306, the statement of the general Security Rule, requires covered entities to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information (EPHI) the covered entity creates, receives, maintains, or transmits;
(e.g. BlackBerry password use policies)
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
(e.g. BlackBerry uses AES and 3DES encryption)
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and
- Ensure compliance by its workforce.
(e.g. BlackBerry IT management policies)

The Security Rule is scalable and technology neutral -- it describes a set of standards and specifications for protecting EPHI but does not specify technological product solutions. Covered entities are allowed to implement technological solutions appropriate to their operations with the only requirement being that organizations support their selected solutions with thorough security assessment and risk analysis in compliance with the Security Rule.

Security Standards

Security standards are divided into categories of administrative, physical and technical safeguards. Each set of safeguards is comprised of a number of standards, which generally consist of several implementation specifications that are either required or addressable. An "implementation specification" is a detailed instruction for implementing a particular Security Rule standard. While required specifications are mandatory as the name suggests, addressable specifications must also be implemented but provide some flexibility to recognize that PHI and EPHI systems vary by organization. "Addressable specifications are not optional. If the covered entity chooses not to implement an addressable specification based on its assessment, it must document the rationale supporting that measure and, if reasonable and appropriate, implement an equivalent alternative measure."ⁱⁱⁱ

1. Administrative Safeguards

In general, this section of HIPAA describes administrative procedures that should be implemented to meet security standards, and includes formal practices for governing the selection and implementation of security measures and the conduct of personnel. The "Chain of Trust" concept is also described and holds that organizations sharing health information with one another must have similar levels of data security to "protect the integrity and confidentiality" of the data communicated.

2. Physical Safeguards

This category focuses on the mechanisms required for the protection of physical computer systems, equipment and the buildings in which EPHI is stored from threats such as fires, natural disasters, environmental hazards, and unauthorized intrusion. Also covered are physical access controls such as locks and sign-in procedures.

3. Technical Safeguards

In general, these are the processes used to protect data and to control access to EPHI. They include authentication controls to verify sign-ons and data encryption to protect integrity and confidentiality of data. Procedures implemented to protect data, as well as to control and monitor information access must comply with these rules. The five technical safeguards are as follows:

A. Access Controls

This standard refers to technical policies and procedures governing information systems that maintain EPHI. Only persons and/or software applications that have been granted access rights should be permitted access. Policies, procedures, and processes must be developed and implemented for electronic information systems that contain EPHI to only allow access to persons or software programs that have appropriate access rights.

Implementation Specifications for Access Controls are:

- Unique User Identification (Required) - A unique name and/or number for identifying and tracking user identity should be assigned to each user.
- Emergency Access Procedure (Required) - Organizations should develop (and implement as needed) procedures for obtaining necessary EPHI during emergencies.
- Automatic Logoff (Addressable) - Organizations should employ electronic procedures that terminate electronic sessions after a predetermined period of inactivity.
- Encryption and Decryption (Addressable) - Organizations should implement mechanisms that encrypt and decrypt EPHI.

B. Audit Controls

This safeguard outlines requirements to implement mechanisms (hardware, software, and/or procedural) to record and examine activity in information systems that contain or use EPHI.

C. Integrity

Policies, procedures, and processes must be developed and implemented that protect EPHI from improper alteration or destruction. Implementation Specifications to ensure Integrity are:

- Mechanism to Authenticate Electronic PHI (Addressable) – Organizations should implement electronic mechanisms to corroborate that EPHI has not been modified or destroyed in an unauthorized manner.

For each addressable implementation specification, a covered entity must do one of the following:

Implement the specification if reasonable and appropriate; or
If implementing the specification is not reasonable and appropriate:

- Document the rationale supporting the decision and
- Implement an equivalent measure that is reasonable and appropriate and that would accomplish the same purpose or
- Not implement the addressable implementation specification or an equivalent alternative measure, if the standard could still be met and implementing the specification or an alternative would not be reasonable or appropriate.

If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity must consider options for implementing it. The decision regarding which security measures to implement to address the standards and implementation specifications will depend on a variety of factors, including:

- The entity's risk analysis – What current circumstances leave the entity open to unauthorized access and disclosure of EPHI?
- The entity's security analysis – What security measures are already in place or could reasonably be put into place?
- The entity's financial analysis – How much will implementation cost?

D. Person or Entity Authentication

This safeguard outlines requirements to develop and implement policies, procedures, and processes verifying that persons seeking access to EPHI are who they claim to be.

E. Transmission Security

This safeguard outlines the development and implementation of technical policies, procedures, and processes necessary to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network (e.g., the Internet or Intranets). Implementation Specifications for Transmission Security are:

- Integrity Controls (Addressable) - Security measures ensuring that electronically transmitted EPHI is not improperly altered without detection until disposed of.
- Encryption (Addressable) - Whenever deemed appropriate, organizations should implement a mechanism to encrypt EPHI.

Table One: Security Standards Matrix (Appendix A of the Security Rule)^{iv}

TECHNICAL SAFEGUARDS			
Standard	Section	Implementation Specifications	
		(R) = Required, (A) = Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)	(R)	
Integrity	163.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)	(R)	
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

Section 2: Mobile Devices in Healthcare

Growing Use of Wireless Devices

Networked wireless devices are increasingly being adopted by healthcare organizations (HCOs) to deliver bottom-line benefits such as improved productivity, improved quality and speed of care, and reduced operating costs. BlackBerry, for example, is being used by various HCOs to:

- Access and update medical forms instantaneously;
- Send electronic prescriptions wirelessly;
- Enable physicians to quickly send and receive medical database information anytime and anywhere; and
- Maintain accurate and timely inventory data.

As handheld capabilities increase -- delivering even more value to organizations -- the corresponding use of mobile devices such as notebooks, PDAs, and BlackBerry devices within HCOs is growing. According to the *16th Annual HIMSS Leadership Survey sponsored by Superior Consultant Company/ACS Healthcare Solutions*, fifty-nine percent of responding healthcare CIOs named PDAs as a technology their organizations planned on implementing over the next two years. A further fifty-one percent of respondents expected their organizations to

adopt Wireless Information Appliances within the next two years. As the functionality and ease-of-use of mobile devices increases, mobile devices are expected to further penetrate the healthcare industry. HIPAA compliance is a core assessment area that must be included as part of the wireless product selection process.

The BlackBerry Enterprise Solution in Healthcare

HIPAA compliance encompasses a covered entity's entire system for exchanging, storing and managing EPHI. Therefore, a healthcare organization's compliance with HIPAA requirements should not be viewed in terms of individual technology solutions being "HIPAA Compliant" (or not) since it is the organization's entire system for transmitting and storing electronic data from the front-end (data capture) to the back-end (data storage) that is assessed as HIPAA compliant. Accordingly, technology solutions should be assessed in terms of how the solutions help the organization to meet HIPAA Security Rule specifications and contribute to a HIPAA compliant system. For example, an e-mail containing EPHI may be sent from a BlackBerry device to a nursing station on a personal computer (PC). The data transported from the BlackBerry device to the BlackBerry Enterprise Server is secure and encrypted but the e-mail stored on the nursing station may be susceptible to theft or unauthorized access if the nursing station PC is left unsecured. In this scenario, the wireless components of the IT system are secure and may be viewed as HIPAA compliant, however the system is non-compliant with HIPAA because the EPHI stored on the nursing station is unprotected.

The BlackBerry solution satisfies HIPAA transmission security requirements because it provides secure end-to-end data transmission from the BlackBerry device to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server also minimizes data vulnerability by acting solely as a conduit between the BlackBerry device and the organization's messaging server. All data passed between the server and the device is stored on the organization's Messaging Server. The BlackBerry solution also embraces the critical cryptographic concepts of encryption and authentication:

1. **Encryption:** crucial to creating confidential messages, encryption is the scrambling of data based on a secret key so that only the parties that know the secret key can decrypt the encrypted data. BlackBerry's end-to-end security relies on Triple-DES or AES to encrypt all data.
2. **Integrity and Authenticity:** Integrity enables a recipient or system to detect if a message has been tampered with in transit while authenticity allows the recipient to identify the sender and trust that the sender actually did send the message. The BlackBerry Enterprise Solution™ encryption mechanism provides integrity and authenticity because decrypted and decompressed messages must conform to a known message format in order to be accepted by the BlackBerry device. Since the value of the encryption key is known only to the BlackBerry Enterprise Server and the BlackBerry device, a recipient will know that a message that does not conform has been altered in transit. The BlackBerry device automatically rejects messages that do not conform to the known message format upon decryption.

In order for a covered entities mobile strategy to comply with the Technical Safeguards stipulated by the Security Rule, a covered entity must devise mobile policies, procedures and processes encompassing its entire system of transmitting, managing and storing EPHI. HIPAA compliance is only achieved if the front-end mobile devices are secure and the back-end is not vulnerable to unauthorized access by third-parties. BlackBerry fits well within a HIPAA compliant environment.

Section 3: Best Practices for Wireless Device Management

Common Wireless Threats and Vulnerabilities

Wireless devices have unique characteristics that expose them to special risks. HCO's should consider these factors in developing policies and procedures to comply with the Security Rule's Technical Safeguards. There are three main privacy and security risks of wireless devices:

Table Two: Common Wireless Device Vulnerabilities

Risk	Description	Solution
Device Content Risk	Data on handheld devices is susceptible to malicious executables (i.e., viruses, worms) and to device corruption or breakdown.	<p>A mix of IT policy and platform choice can mitigate this risk. BlackBerry, for example, mitigates these risks through its design features:</p> <ul style="list-style-type: none"> BlackBerry IT policy allows for strict device configuration management so that only authorized applications can be run on BlackBerry devices. The BlackBerry Attachment Service protects devices against macro viruses by using an abstracted data format to interpret, convert and preserve the format of e-mail attachments. Content protection can be enabled on BlackBerry handhelds in order to encrypt data stored on the handheld using 256-bit AES. IT policy can be used to enable content protection.
Unauthorized Intrusion Risk	Wireless devices are vulnerable to network intrusion. Unauthorized third-parties can hack into unprotected networks to sniff accounts and passwords using them to break into the network and acquire unauthorized server control.	<p>BlackBerry supports strong passwords with wireless IT policy support to enforce their use.</p> <p>BlackBerry only communicates through the firewall on an outbound connection basis via port 3101. No inbound connections and inbound firewall reconfigurations are required.</p> <p>BlackBerry also uses strong encryption (AES and 3DES) to best guarantee the privacy of data during transmission.</p>
Data Integrity, Confidentiality, and Authenticity Risk	In many wireless implementations, data travels from mobile device to access point without being checked for integrity; and is then forwarded without being authenticated. Unauthenticated data access and manipulation may allow intruders to compromise data.	A mobile solution should authenticate traffic between devices and the server to ensure that only authenticated data is accepted. BlackBerry, for example, authenticates all data exchanged between the BlackBerry Enterprise Server and BlackBerry devices to ensure that unauthorized third parties do not compromise the data.

Authentication Methodologies

Authentication is a core component of network security and "Person or Entity Authentication" is a required standard of the Security Rule. Security audits expect access to be restricted by at least two of three possible authentication methodologies:

Table Three: Authentication Methodologies

Authentication Methodology	Definition	Technology
Single-factor authentication	"Something you know"	Password, key phrase
Two factor authentication	Single factor authentication plus "Something you have"	Swipe card, token, key fob, etc
Three-factor authentication	Two-factor authentication plus "Something you are"	Biometrics (e.g., fingerprint, voice recognition, iris or retinal scan)

Single-Factor Authentication

“Single Factor” authentication is the simplest form of authentication, consisting of a password, i.e., a user identifies herself by providing “something they know”. Passwords provide an acceptable level of security for many applications, with the weakness being that a compromised password is all an unauthorized third-party requires to gain access to a system. Accordingly, best practices strive to harden passwords by making them difficult for unauthorized individuals to acquire.

Two-Factor Authentication

Two-factor authentication combines a password (“something you know”) with a hardware or software token (“something you have”) to create a more secure authentication procedure. An unauthorized party would require both the password and the token to access the system; a significantly more difficult task. Hardware tokens include cards and key fobs, which are used in conjunction with a Personal Identification Number (PIN). Smart cards, which are credit card-sized plastic cards embedded with circuit chips that provide memory capacity and processing capability, are common hardware tokens. Both hardware and software tokens are available for use with wireless handhelds. BlackBerry, for example, can be enabled for two-factor authentication by adding the BlackBerry Smart Card Reader. The BlackBerry Smart Card Reader is a lightweight, wearable smart card reader that allows controlled access to BlackBerry devices via Bluetooth® technology and advanced AES-256 encryption. Administrators gain additional control over the wireless environment through the ability to wirelessly manage the lifetime of the security keys on the BlackBerry Smart Card Reader.

Single Factor Authentication: Password Best Practices

Passwords should use mixed-case letters and alphanumeric characters including punctuation. BlackBerry administrators can force users to create robust passwords by rejecting excessively repetitious or simplistic passwords such as those consisting of a natural sequence (such as 1, 2, 3, 4, 5) or identical characters.

Passwords should be at least eight characters long – the longer the password the harder it is to guess or to crack. For example, BlackBerry users can set individual passwords between 4 and 14 characters long, with IT administrators having the ability to specify the length and composition of a password.

Passwords should be changed regularly. BlackBerry system administrators can set device policies specifying the length of time that user device passwords can exist before becoming invalid, thereby forcing users to routinely update their passwords. BlackBerry administrators can also enforce how long a user’s device can remain open after last use before it locks automatically.

Access to devices can be controlled via passwords. The BlackBerry device, for example, only stores a hash of the password on the device. This hash (SHA1) is a one-way function that converts the password into a numerical representation of the original and cannot be reversed to reveal the password. The BlackBerry further employs mechanisms to ensure that only properly authorized and authenticated applications can access the hash value.

Three-Factor Authentication

Biometrics utilize a physical characteristic (e.g., a fingerprint) to provide the third authentication factor (“something you are”) for user identification. In the United States, biometric technology is a critical component in the Federal government’s implementation of a standard identification credential for Federal workers and contractors in compliance with Homeland Security Presidential Directive 12 (HSPD-12). Although the prices of biometric technologies have been reduced significantly, companies are still striving to develop reliable and secure technologies at price points appropriate for the majority of corporate customers. Biometrics is available for mobile devices and in the future, biometrics may become a standard part of two-factor authentication (e.g., a fingerprint pressed into a card in lieu of a PIN). Currently however, two-factor authentication (“something you know” and “something you have”) is the industry standard in terms of advanced authentication solutions.

Most organizations, including governmental organizations, trust the degree of password protection provided by BlackBerry and consider this sufficient as an intruder must steal a registered users device and know the password.

Mitigating Wireless Vulnerabilities

Industry experience suggests that a combination of appropriate technology and IT security policies and procedures can assist organizations in mitigating wireless device vulnerabilities. Industry best practices suggest the following recommendations for securing wireless devices:

1. Develop security policies and procedures for mobile devices, including provisions for the use of personally owned devices. Areas of consideration include;
 - a. Protection against unauthorized users: User authentication is a core component of any security system. Authentication should be performed at both the handheld level and the network server level.
 - b. Protection of data transmissions: Data exchange must be secure from end-to-end, especially on public networks. Mobile solutions should operate on secure connections for both data synchronization and client/server communications.
 - c. Protection of data on lost devices: Mobile devices are prone to loss; if an unauthorized person gains possession of a device they should be unable to access its data.
 - d. Protection of mobile assets: Centralized administration should be used to safeguard mobile assets. For example, system administrators should enforce password policies to ensure mobile users are following established procedures (e.g., routinely changing passwords.)
2. Identify the organization's mobile device users
3. Ensure end-user acceptance and a balanced policy (security vs. ease-of-use) by consulting with end-users during development and initial implementation of security procedures.
4. Implement mobile security solutions that integrate with existing enterprise solutions to simplify the administration of security policies and users. For example, all e-mail messages between the organization's e-mail server and mobile devices that are outside the firewall should be encrypted.
5. Implement and enforce mobile device security policies, including mandatory access control and data encryption. Possible guidelines for mobile devices might include:
 - Mobile wireless devices containing confidential information should utilize user authentication and data encryption;
 - Laptop/notebook computers containing confidential information should employ user authentication and data encryption when they are subject to heightened risk of loss or theft.
 - Mobile devices should be set up to power-on with a password to protect confidential data in a case of loss of the device.

BlackBerry devices are designed for corporate security best practices, offering comprehensive security features at both the system administrator and device levels. For example, using wireless IT commands, system administrators can immediately respond to lost or stolen devices and protect confidential enterprise information, including the following commands:

- **Wipe Device:** If a BlackBerry device has been stolen or cannot be found, the system administrator can erase all information and application data stored on the BlackBerry device remotely.
- **Set a Password and Lock the Device:** The system administrator can create a new password and lock the device remotely.
- **Reset the Password and Lock the Device:** If the user has forgotten the device password, the system administrator can reset the password remotely and communicate the new password to the user.

At the device level, BlackBerry contains multiple features designed to conform to enterprise security best practices:

- System administrators through the use of IT policy can force password use.
- The IT administrator or user can also specify a security timeout, setting the number of idle minutes that occur before the device locks so that data stored on the device remains safe in the event of a theft or loss.
- The IT administrator can force a periodic security challenge that will require the user to enter a password 60 minutes after unlocking a device. This challenge happens regardless of the level of activity on the device and is designed to minimize the window that an unlocked device can be used.
- By default, a user is limited to ten password attempts on the BlackBerry device. The data on the device is deleted after ten incorrect password attempts. An administrator can reduce or increase the number of incorrect login attempts in order to meet existing corporate security policies for unsuccessful login attempts.
- System administrators can change the value of the password setting through an IT policy.
- Users can enable a device application that encrypts all data on the local data store so violators cannot get at data by physically removing the memory. IT managers can wirelessly enforce the use of this feature.

BlackBerry and HIPAA Technical Safeguards Best Practices

HCOs are free to implement any technology that allows the organization to comply with HIPAA's Security Rule Technical Safeguards. The BlackBerry solution assists HCOs in meeting Security Rule requirements by providing features that meet Implementation Specifications detailed by the Security Rule, i.e., encryption, authentication services, and data integrity. Table Three details best practices for implementation of Security Rule implementation specifications and where the BlackBerry solution contributes to compliance.

Table Four: Security Rule Standards Best Practices for Implementation

Technical Safeguard	Implementation Specification	Best Practices For Implementation	BlackBerry Feature or System Component
A. Access controls	Unique user identification	Authentication Services	Unique device encryption key
A. Access controls	Emergency access procedure		911 access even when device is locked
A. Access controls	Automatic logoff	Configurable Idle Timeout	Time-based device lockdown
A. Access controls	Encryption and decryption	Triple-DES or Advanced Encryption Standard (AES)	End-to-end encryption protocol
B. Audit Controls	Record and examine activity	Real-time Monitoring	BlackBerry Enterprise Server
		Logging and Alerting	BlackBerry Enterprise Server
C. Integrity	Mechanism to authenticate electronic PHI	Unique Session Keys	BlackBerry message authentication
C. Integrity	Integrity controls	Triple-DES or Advanced Encryption Standard(AES)	End-to-end encryption protocol
		Authentication services	BlackBerry message authentication
		Unique Session Keys	BlackBerry Enterprise Server
D. Person or Entity Authentication	Unique user identification	Authentication services	Enforceable strong passwords
E. Transmission Security	Encryption and decryption	Triple-DES or Advanced Encryption Standard (AES)	End-to-end encryption protocol
E. Transmission Security	Integrity controls	Advanced Encryption Standard(AES)	End-to-end encryption protocol
		Authentication services	BlackBerry message authentication
		Unique Session Keys	BlackBerry Enterprise Server

Conclusion

HIPAA compliancy with respect to the Security Rule pertains to the covered entity's IT system as a whole and cannot be applied to a singular part of the organization's IT systems. For example, while the BlackBerry provides advanced password security features and access controls, and uses Triple-DES or AES to encrypt all data transmitted between the Black Berry device and BlackBerry Enterprise Server, a HIPAA covered entity's system will not be deemed HIPAA compliant if its data servers or PCs do not possess adequate authentication and data protection controls and render data vulnerable to access by unauthorized third-parties.

The technical safeguards described by HIPAA's Security Rule are necessary to protecting an entity's systems and data from unauthorized access. They may be viewed as standard IT security policies that should be followed and implemented even without the requirements of HIPAA, if deemed reasonable and appropriate to an entity's environment (i.e., systems should possess authentication controls as a security requirement).

Therefore, in addition to evaluating a wireless solution in terms of its core capabilities, a covered entity should also assess a wireless solution on the basis of the solution's security features and the solution's readiness, operability and applicability for seamlessly integrating its security-feature set into a fully HIPAA compliant environment.

The BlackBerry solution provides a secure front-end in terms of the BlackBerry device and a back-end that minimizes potential security issues (i.e., data is not stored on the BlackBerry Enterprise Server). At the front-end, the BlackBerry device features strong authentication and encryption features, and during transmission, all data exchanged between the BlackBerry Enterprise Server and the device is encrypted (using AES or Triple DES encryption). Whether email, calendar appointments, or corporate applications data like accessing a drug interactions database, BlackBerry uses the same secure pipe for all forms of data.

BlackBerry may be considered as possessing the features and attributes needed to meet the standards of a covered entity's fully HIPAA compliant information system. Organizations looking to install BlackBerry may pursue the benefits of BlackBerry without unduly exposing themselves to the challenges being presented by HIPAA.

APPENDIX ONE – BLACKBERRY SECURITY MODEL

BlackBerry Enterprise Server Architecture

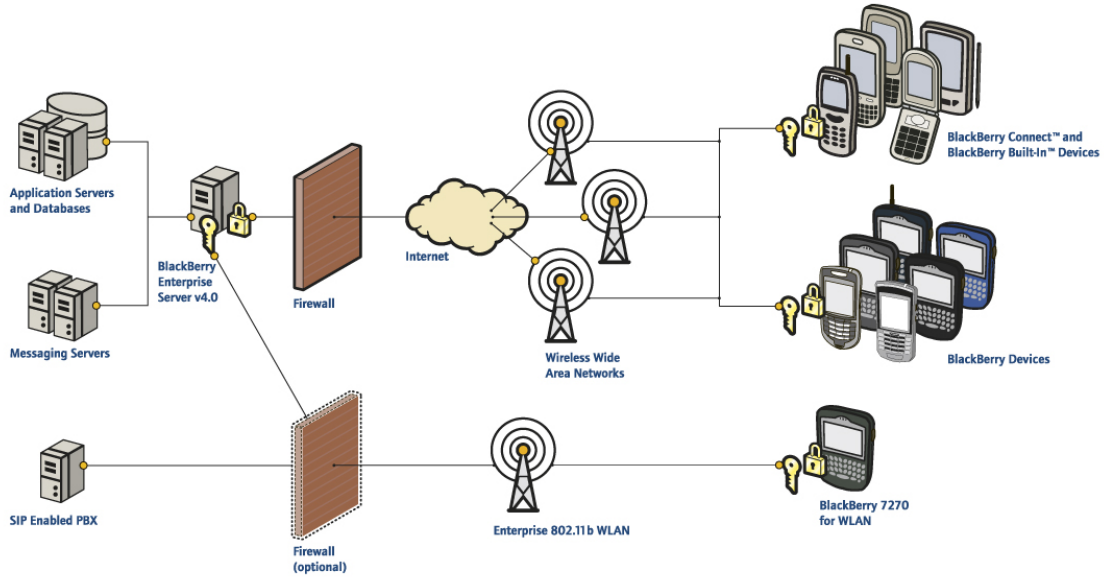
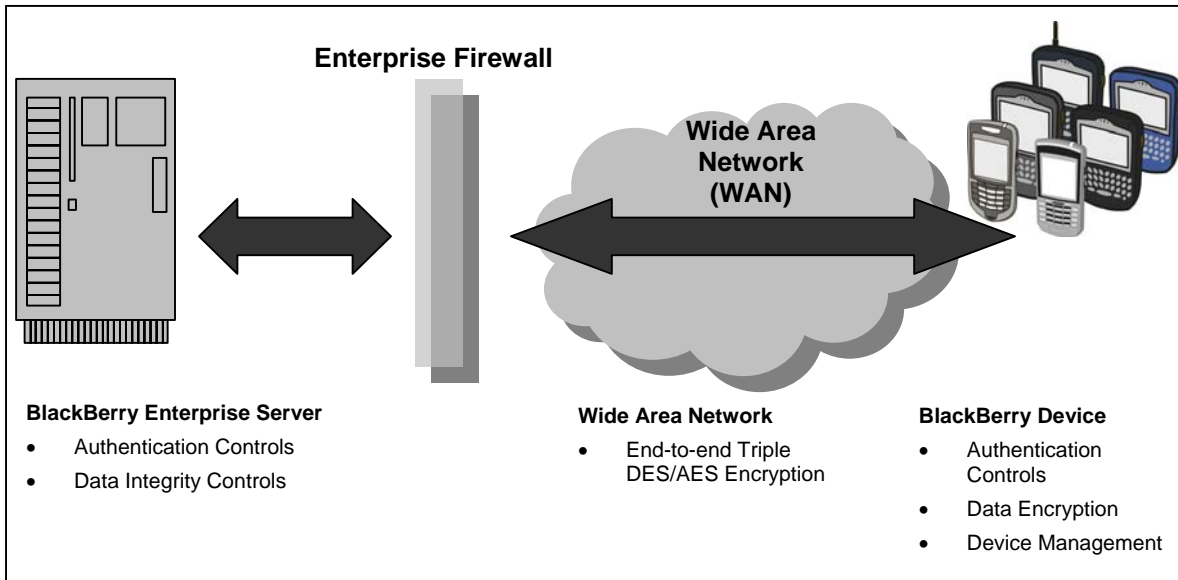


Diagram 1: BlackBerry Enterprise Server Architecture

Diagram 2: BlackBerry Solution Security Layers



Encryption and Authenticity

The BlackBerry Enterprise Solution has been developed with data security as an integral feature including data encryption, integrity and authenticity as core components. The BlackBerry solution safeguards the integrity, confidentiality and authenticity of enterprise data by keeping data encrypted from behind the firewall through to the BlackBerry device and visa versa. Diagram 2 illustrates BlackBerry security layers for device, transmission and server security.

End-to-end Wireless Encryption

All data transmitted through the BlackBerry solution is encrypted; data is never decrypted outside the corporate firewall. The BlackBerry Enterprise Solution offers two transport encryption options, AES and Triple DES, for all data transmitted between the BlackBerry Enterprise Server and the BlackBerry device, using symmetric key cryptography to protect the confidentiality of data. Before sending a message, the device encrypts the message using a key unique to that device (the master encryption key). When receiving a message from the device, the BlackBerry Enterprise Server decrypts and decompresses the message using the master encryption key. The device, the user's mailbox, and the BlackBerry Enterprise Server configuration database each store the master encryption key.

Administrators can enable data encryption using either a Triple-DES encryption key or an AES encryption key. Using the Triple-DES Encryption Standard, BlackBerry uses three iterations of the Data Encryption Standard (DES) algorithm. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. With Triple-DES, the data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the first key. The Advanced Encryption Standard (AES) was developed to replace the Data Encryption Standard (DES) and provides a newer combination of security and performance than DES or Triple-DES. AES can provide greater security against brute-force attacks by offering a larger key size. With AES BlackBerry uses 256-bit keys to encrypt data that is sent between the BlackBerry Enterprise Server and the device.

BlackBerry Enterprise Server Permits Only Trusted Connections

The BlackBerry Enterprise Server does not store any e-mail or data and only communications that can be decrypted with a valid encryption key are permitted between the server and the wireless network. To increase protection from unauthorized parties, there is no staging area between the server and the BlackBerry device where data is decrypted. To further enhance the security of the solution, the BlackBerry Enterprise Server allows only authenticated, outbound-initiated connections through port 3101 of the firewall. Unauthorized commands cannot be executed on the system because no inbound traffic is permitted from sources other than the BlackBerry device or the organizations e-mail server.

HTTPS for Secure Data Access

The Mobile Data Service (MDS) feature of the BlackBerry Enterprise Server acts as a secure gateway between the wireless network and corporate intranets and the Internet. Leveraging the Triple DES or AES encryption transport for BlackBerry, MDS also enables HTTPS connections to application servers. BlackBerry devices support HTTPS communication in Proxy Mode (an SSL/TLS connection is created between the BlackBerry Enterprise Server and the application server on behalf of the BlackBerry device) and in End-to-End Mode (data is encrypted over SSL/TLS for the entire connection between the BlackBerry device and the application server) depending on corporate security requirements.

S/MIME Support

BlackBerry has optional support for the S/MIME (Secure Multipurpose Internet Mail Extensions) data protection protocol. The BlackBerry S/MIME Support Package leverages an organization's

existing S/MIME capabilities, enabling BlackBerry users to store and retrieve private and public keys, in order to read, sign and encrypt S/MIME messages. With S/MIME, encryption is end-to-end from sender to recipient including encryption over the company's intranet. Without S/MIME BlackBerry encryption extends from behind the firewall to the device. Most companies using BlackBerry consider the latter model sufficient.

Strong IT Policy Enforcement and Management for BlackBerry Devices

BlackBerry extends corporate security to the device level by providing administrators with comprehensive security management tools. Customizable IT policies can be used to make password authentication mandatory, and enforce local encryption of all data (messages, address book entries, calendar entries, memos and tasks). By default, password authentication is limited to ten attempts after which the device's memory is erased. Additionally, system administrators can remotely change device passwords, and lock or delete information from lost or stolen devices using wireless commands. They can also enforce the encryption of data on the device's local memory store to safeguard against physical tampering.

Certified Secure

BlackBerry devices feature advanced encryption technology. As a result, BlackBerry devices have received the Federal Information Processing Standard (FIPS) 140 certification, signifying their adherence to strict government security standards. FIPS 140 is a US government standard providing a benchmark for implementing cryptographic software, specifying best practices for implementing crypto algorithms, handling key material and data buffers, and working with the operating system. FIPS 140 validation is an additional proof done by a third party showing a security software implementation to be of the highest quality and standards.

Independently Audited Security Model

All aspects of the BlackBerry security model have been audited and verified by @stake Inc., a leading digital security-consulting firm. @stake Inc.'s analysis indicates that "the BlackBerry security model provides the same level of security as a traditional VPN connection" and that "the BlackBerry security model provides the necessary confidentiality, integrity, and authentication"^{vi}.

Java-based BlackBerry Devices

The BlackBerry device addresses security concerns over third-party applications operating through the BlackBerry Java Development Environment (JDE) open and flexible framework for application development in the following ways:

- Third-party applications can only access persistent storage or user data, or communicate with other applications, through specific application programming interfaces (APIs).
- Applications that use these sensitive APIs must be digitally signed by RIM.
- Administrators can restrict privileges of each third-party application.

Sensitive APIs on the BlackBerry device are controlled by "code signing"; third-party applications using these APIs must be digitally signed by RIM before they can be installed and run on a BlackBerry device, thereby preventing malicious applications from accessing data on the device. Code signing also provides an audit trail of applications that use sensitive APIs. RIM does not inspect or verify third-party applications as "code signing" ensures that only trusted and legally accountable parties can deliver applications. However, system administrators can block third-party applications from being loaded on the device by using IT policy.

Bluetooth Support on BlackBerry Devices

The BlackBerry device's Bluetooth functionality supports voice profiles (i.e., wireless handsfree headset and car-kit) and data (i.e. smart card). Administrators have full control over Bluetooth functions by using IT policies to provide granular control over the Bluetooth capabilities on a BlackBerry. For example, administrators can prevent BlackBerry handhelds from establishing

connections to other Bluetooth enabled devices. Bluetooth functions for BlackBerry are disabled by default and system administrators can enforce this by using IT policy.

Whereas most wireless devices utilize Bluetooth modules powered by supplies unconnected to the device's main chipboard, BlackBerry's Bluetooth module is connected directly to the BlackBerry device's main processor. Therefore, when Bluetooth is disabled on the BlackBerry device, the entire Bluetooth module is cut off from the main processor, eliminating any chance of unauthorized third-party access from Bluetooth to the main BlackBerry processor.

Deleting Device Data

Users have the ability to delete all device data. Device data is also automatically deleted from the device after ten incorrect password attempts (default IT policy setting). When data is deleted from the device, master encryption keys, content protection keys, and passwords are also deleted but IT policy is not deleted from the device.

Password Keeper

Users can create and store all their passwords in the Password Keeper. The first time users open the password keeper, they must create a password keeper password. Information in the password keeper is encrypted with 256-bit AES. Information stored in the password keeper is only decrypted when users type the password keeper password. Users can also generate random passwords and copy passwords to the clipboard in the password keeper. Device data is automatically deleted from the device if the password keeper password is entered incorrectly ten times.

Attachments

The BlackBerry device supports attachments through the BlackBerry Attachment Service. The BlackBerry Attachment Service uses a proprietary data format to interpret, convert, and preserve the format of email attachments without sending native files that can convey viruses to the device. The Attachment Service supports Microsoft Excel, Microsoft PowerPoint, Corel® WordPerfect®, Adobe® PDF, and text documents. Attachment data is protected in the following ways:

- Encryption: All Attachment Service data sent from the BlackBerry Enterprise Server to the device is encrypted.
- Data exchange behind firewall: The Attachment Service communicates with the BlackBerry Enterprise Server directly over a TCP/IP connection. No inbound or outbound connections through the firewall are required.
- Virus avoidance: Because the Attachment Service does not require the applications used to create the email attachments, the BlackBerry Enterprise Server and devices are protected against infection by macro viruses.

Focus on Corporate Features for Added Security

BlackBerry devices are high-performance wireless tools for business users. BlackBerry devices do not include consumer-oriented features such as built-in digital camera, digital music player (i.e., MP3 player) or native file support (e.g., ability to support file attachments in their native format). These features significantly reduce battery life and pose additional security issues at the device and corporate policy levels (for example, the potential use of built-in digital cameras in sensitive or restricted areas). BlackBerry devices deliver high-performance wireless communications capabilities without compromising essential security functionality. For companies without policies restricting the use and availability of features such as digital cameras, video recorders and music players, BlackBerry Connect™ and BlackBerry Built-In™ devices available from other handset manufacturers can be used to provide a more secure and richer e-mail, calendar and applications access experience.

Table Five: BlackBerry Corporate Feature Focus

Feature	Weakness	Conclusion
Camera	Increasingly banned or restricted – businesses, government offices, courtrooms, fitness centers, healthcare facilities, retail outlets, entertainment venues (concerts), and spas are some of the initial locations to ban or restrict camera-phones on their premises.	The appeal of camera-phones varies substantially by end user and has lowest appeal with business users. BlackBerry does not include an integrated camera because business users need to be able to carry their BlackBerry device everywhere they go throughout their day
MP3 Player	Large memory capacity and power-hungry processors are required to support MP3 playback. These hardware considerations significantly reduce the battery life of the mobile device.	BlackBerry devices are high performance wireless tools for business users
Native File Support	Ability for a device to support attachments and or applications in their native format Native files can host viruses which can be deposited onto company networks along with infecting the mobile device. Mobile viruses on Symbian and WinCE devices began appearing during the summer of 2004.	BlackBerry includes highly functional attachment viewing that does not expose the device or other business systems to viruses. While the convenience of being able to edit on the device is an attribute for some, most users prefer to wait until they have returned to their desktop or laptop to edit documents. BlackBerry's attachment viewing technology minimizes over-the-air data transfer requirements thereby minimizing cost while promoting end user performance

IT Policies for Security Settings

IT policies enable system administrators to customize the features such as password, mail forwarding, and browser options common to all BlackBerry device users on a given BlackBerry Enterprise Server. IT policies provide an efficient method for managing many different users simultaneously. Using the BlackBerry Enterprise Server, system administrators can set specific IT policies to define how users use the security settings that are included on BlackBerry devices and in the BlackBerry Desktop Manager.

- IT policies for security: All BlackBerry user security settings can be defined by system administrators. For example, system administrators specify whether a password is required, the length of time that a password can exist before it becomes invalid, and the length and composition of a password. Encryption key details can also be specified using an IT policy.
- Wireless policy deployment: All IT policies, including security settings, can be immediately applied wirelessly. To accomplish wireless delivery of new policies and immediate user adoption, IT policy settings are automatically written to the user configurations. To verify that the settings are always current, the BlackBerry Enterprise Server periodically transmits device settings to the device wirelessly.
- Continuous updating of IT policies: All IT policies, including security settings, are updated regularly. The BlackBerry device is updated periodically through wireless policy deployment. With continuous updating, BlackBerry users quickly adopt new IT policies, including security settings.
- Group policies: The IT policy feature enables a system administrator to define a policy for a group and apply it to all users in the group instead of creating a policy for each user. For example, a system administrator can create a policy for executives, and assign each executive to the group policy.

Sources

Phoenix Health Systems, www.hipaadvisory.com

Mobile Healthcare Alliance Website, www.mohca.com

“Security 101 for Covered Entities”, published by the Centers for Medicare & Medicaid Services

“Strong PDA policies help secure data and prevent equipment loss”, Suzanne Thornberry, TechRepublic

Resources

Complete HIPAA information is located at: <http://www.hhs.gov/ocr/hippa>

End Notes

ⁱ 16th Annual HIMSS Leadership Survey sponsored by Superior Consultant Company/ACS Healthcare Solutions, 2004

ⁱⁱ Field Guide to HIPAA Implementation, published by the American Medical Association

ⁱⁱⁱ “Security 101 for Covered Entities”, Centers for Medicare & Medicaid Services

^{iv} *ibid*

^v “Strong PDA policies help secure data and prevent equipment loss”, Suzanne Thornberry, TechRepublic

^{vi} @stake BlackBerry security assessment

The RIM and BlackBerry families of related marks, images and symbols are the exclusive properties and trademarks of Research In Motion Limited-used by permission. BlackBerry and “Always On, Always Connected” are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.