BlackBerry

White Paper

BBM Enterprise and HIPAA

Executive Summary

The Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the federal regulations published at 45 CFR Parts 160 and 164 and the federal regulations (collectively, "HIPAA"), 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 leaves your options for compliance wide open, providing technology-neutral implementation specifications and no formal certification process.

Under such a broad regulatory regime, BlackBerry® is the right service provider to handle your electronic protected health information (ePHI). BBM® Enterprise allows for real-time collaboration with the following compliant features: encryption, authentication services, data integrity and authentication, and auditing. BlackBerry develops healthcare workflows and features for BBM Enterprise hand-in-hand with healthcare customers.

Administrative and physical safeguards

In managing your risk regarding administrative and physical safeguards, you need to work with trustworthy third parties.

A leader in mobile security, BlackBerry builds every layer of its products with certified security features such as TLS, FIPS, AES, as well as BlackBerry proprietary security technology that has stood the test of long-time enterprise use. In managing the BlackBerry security environment, BlackBerry follows best practices such as risk management, data backup, disaster recovery, and strict access control. The BlackBerry security solutions are the only ones trusted enough for global financial services companies, top law firms, health care providers, law enforcement, defense departments, and the Oval Office. BlackBerry has over 80 security certifications and approvals, more than any other mobile vendor.

Table 1. How the BBM Enterprise solution contributes to HIPAA compliance

BBM Enterprise feature or system component	HIPAA technical safeguard standard
End-to-end Encryption Protocol	• Access Controls • Integrity • Transmission Security
Unique Encryption Key	• Access Controls • Integrity • Person or Entity Authentication • Transmission Security
BlackBerry Message Integrity and Authentication	• Integrity • Person or Entity Authentication
BlackBerry Audit and Archiving Service	• Audit Controls

Technical safeguards

The BBM Enterprise solution possesses security features and capabilities enabling it to operate within a HIPAA compliant environment. BBM Enterprise message content is configured so that even BlackBerry cannot decrypt it.

1 HIPAA Security Series "Security 101 for Covered Entities", Centers for Medicare & Medicaid Services
2 See HIPAA Security Series, Appendix A.

Introduction

HIPAA security standards

The HIPAA Security Rule standards are divided into three categories: administrative, physical, and technical safeguards. Each set of safeguards is comprised of "implementation specifications" that are either required or addressable. While required specifications are mandatory, addressable specifications must also be implemented but they provide flexibility to recognize that systems vary by organization.[1]

1. Administrative Safeguards.

In general, this HIPAA section describes administrative procedures that should be implemented to meet security standards. The "Chain of Trust" concept is described, which suggests 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 that are required to protect physical computer systems, equipment, and the buildings in which ePHI is stored, from threats such as fires, natural disasters, environmental hazards, and unauthorized intrusion.

3. Technical Safeguards.

In general, technical safeguards are the processes used to protect data and to control access to ePHI. They include authentication controls to verify log-in credentials, and data encryption to protect integrity, and confidentiality of data. Procedures implemented to protect data and control and monitor information access must comply with these rules.

4. Breach Notification.

The HIPAA Breach Notification Rule, which incorporates the breach notification requirements introduced by HITECH, requires that notification is provided when a breach of impermissible use or disclosure of protected health information occurs.

Table 2. Security standards matrix[2]

Technical safeguards			
Standard	**Section**	**Implementation specifications, (R) Required, (A) Addressable**	
Access Control - Only allow access to persons or software programs that have appropriate access rights	164.312(a)(1)	Unique User Identifications	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls - Mechanisms (hardware, software, and procedural) to record and examine activity	164.312(b)	-	(R)
Integrity - Protect ePHI from improper alteration or destruction	163.312(c)(1)	Mechanism to Authenticate ePHI	(A)
Person or Entity Authentication - Verify that persons seeking access to ePHI are who they claim to be	164.312(d)	-	(R)
Transmission Security - Guard against unauthorized access to ePHI that is being transmitted	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

Implementing a compliant healthcare program

BlackBerry offers a business associate agreement

BlackBerry is committed to supporting a HIPAA compliant environment, where BBM Enterprise and other solutions can assist you in meeting the law's requirements. To make sure that ePHI will be handled with appropriate safeguards, BlackBerry will enter into a standard business associate agreement that defines and limits how BlackBerry can handle ePHI, and specifies responsibilities for HIPAA compliance. Customers can use BBM Enterprise to send or receive communications between a patient and a healthcare provider after a business associate agreement is signed.

HIPAA provides an exception for service providers that qualify as a "conduit" having no access "other than on a random or infrequent basis" as described in Federal Register, Vol. 78, No. 17, 5571-5572. Because there is no official HIPAA compliance certification, parties can claim the conduit exception without upfront oversight. Even though BlackBerry cannot decrypt BBM Enterprise message content and may qualify for this exception, BlackBerry uses business associate agreements to provide an additional level of compliance assurance to BlackBerry customers.

HIPAA program covers an entire system of policies, procedures, and processes

In order for a healthcare organization's mobile strategy to comply with the Technical Safeguards stipulated by HIPAA, the organization must devise mobile policies, procedures, and processes that encompass its entire system of transmitting, managing, and storing ePHI. It is not enough for one part of the system to be compliant while another is not. That is, an organization's compliance with HIPAA should be viewed as its entire system for transmitting or storing electronic data from the front-end (data capture) to the back-end (data storage). An organization's compliance should not be viewed in terms of an individual technology solution being "HIPAA Compliant" (or not).

To maintain HIPAA compliance for ePHI sent by BBM Enterprise and stored on a device, an organization should institute safeguards for device use and management. A mobile device management solution can secure or "harden" the device on which the BBM app resides. Such management solutions can, for instance, require use of a local non-portable data store and protect against the risk of loss through copy and paste functionality. Management solutions can also impose IT policies, for example, that lock down a device after a certain period of time or allow for the remote lock down or wipe of all information on a lost device. In addition, an organization's usage policies can place responsibility on individuals to prevent unauthorized access and ensure that data is only transmitted and stored securely. Such device safeguards further support compliance with industry standards, such as NIST 800-11. The BlackBerry The Definitive Guide to Enterprise Mobile Security further discusses strategies and tactics for safeguarding your data in a mobile environment.

But the bottom line for you and your healthcare organization is as follows: the risks are too great to leave mobile security to chance, and you and your users no longer have an excuse for not using best practices to protect ePHI and other personal data on mobile devices. As illustrated in the BlackBerry Mobile Healthcare eBook – Strategies, Tactics and Case Studies, BlackBerry has a full suite of containerization, secure file sharing, crisis communications, and enterprise mobility management solutions, not to mention the knowledge, experience, and solutions you can depend on.

BBM Enterprise solution in healthcare

BBM Enterprise fits well within a HIPAA compliant environment with features such as end-to-end encryption, authentication services, data integrity and authentication, and auditing—as well as other healthcare workflows and features.

Administrative and physical safeguards

In considering your risks regarding administrative and physical safeguards, a key factor involves the trustworthiness of third-parties you allow to handle your data. The BlackBerry Corporate Infrastructure Security Overview document describes BlackBerry security practices, explaining why customers that require absolute confidence in the security of their data choose BlackBerry .

The BlackBerry Advanced Assurance team can support your planning, deployment, and compliance lifecycle from beginning to end. With a strong grounding in HIPAA guidance and best of breed standards, BlackBerry offers a varied catalogue of industry-specific services geared to keeping information accessible, secure, and above all, private without ever interrupting the demanding pace of the healthcare industry.

Technical safeguards

BBM Enterprise solution[3]

The BBM Enterprise solution, consisting of protected chats and the BlackBerry® Audit and Archiving Service (BAAS), provides end-to-end message encryption from the time a BBM Enterprise user sends a message to when the recipient receives the message. BAAS provides message archiving for monitoring and logging. And all chats using BBM Enterprise are protected. Even communications with users who do not subscribe to BBM Enterprise receive full BBM Enterprise encryption. This safeguard allows you to securely message patients and healthcare providers in other facilities, even if they only use consumer-grade BBM.

BBM Enterprise standards and algorithms

BBM Enterprise uses FIPS 140-2 validated cryptographic libraries to ensure that it satisfies the security requirements for protecting unclassified information as defined by the Federal Information Processing Standards (FIPS).

BBM Enterprise uses ECC because it offers significant advantages over the most widely used alternative, RSA. BlackBerry uses the ECC implementation that is offered by Certicom, which is a wholly owned subsidiary of BlackBerry. Certicom has been developing standards-based cryptography for over 25 years. Certicom is the acknowledged worldwide leader in ECC, offering the most security per bit of any known public key scheme. For example, a 160-bit ECC key and a 1024-bit RSA key offer a similar level of security. A 512-bit ECC key provides the same level of security as a 15,360-bit RSA key.

BBM Enterprise standards

BBM Enterprise uses the following standards for signing, encrypting, and hashing that meet or exceed the NIST Suite B cryptographic guidelines:

- Digital signature standard FIPS 186-4: Provides a means of guaranteeing the authenticity and non-repudiation of messages
- AES symmetric encryption standard FIPS 197: Uses agreed symmetric keys to guarantee the confidentiality of messages
- HMAC standard FIPS 198-1: Based on SHA2-256 and uses agreed symmetric keys to guarantee the integrity of messages
- Cryptographic key generation standard NIST SP 800-133: Generates the cryptographic keys that are needed to employ algorithms that provide confidentiality and integrity protection for messages
- Secure Hash standard FIPS 180-4: Provides preimage and collision-resistant hash functions that are required for secure HMACs, digital signatures, key derivation, and key exchange

BBM Enterprise algorithms and functions

To protect the connection between BBM Enterprise users during a chat, BBM Enterprise users exchange public signing and encryption keys using an out-of-band shared secret and EC-SPEKE. These keys are then used to encrypt and digitally sign messages between the devices.

BBM Enterprise uses the following algorithms that are based on NIST standards with 256-bit equivalent security:

- EC-SPEKE: Securely exchanges a symmetric key by protecting the exchange with a password
- KDF: Securely derives message keys from shared secrets
- One-Pass DH: Using one user's private key and another user's public key, derives a new shared secret between the users

BBM Enterprise implements the following algorithms and associated key strengths:

- AES-256 for symmetric encryption
- ECDSA with NIST curve P-521 for signing
- One-Pass ECDH with NIST curve P-521 for symmetric key agreement
- SHA2-512 for hashing and key derivation
- SHA2-256-128 HMAC for message authentication codes

BBM Enterprise voice and video calling uses SRTP media streaming and implements the following algorithms and associated key strengths:

- AES-128 in CTR mode for symmetric encryption
- 112-bit salting keys
- BBM Enterprise messaging for symmetric key transfer
- SHA1 80-bit tag for message authentication and integrity

Database Encryption

On iOS and Android devices, the BBM database is encrypted. To encrypt the BBM database, BBM uses SQLCipher, initialized with a passphrase. BBM asks the iOS or Android device for a block of random data (48 bytes) to use as the passphrase. The passphrase is random, unique to each BBM app, and used each time the BBM app starts on a device. BBM encrypts the passphrase and stores it in the device's keystore.

BlackBerry Audit and Archiving Servic

BAAS archives all data passing between devices using BBM Enterprise functionality. This functionality provides the capability for IT departments to meet auditing and archiving requirements. Using BAAS, you can request communications about a certain patient from a specific provider, or a certain term such as a drug name.

The BBM Enterprise security online manual contains more information about how BBM Enterprise protects messages.

[3]This discussion applies to (a) BlackBerry 10 devices running OS 10.3, and BBM version 10.3.30 or later, assigned to BBM Enterprise in the Enterprise Identity administrator console; and (b) Android™ devices running Android 4.0 Ice Cream Sandwich and iOS devices running iOS7 or later using BBM version 2.6 or later. The devices must be assigned to BBM Enterprise by the BlackBerry Enterprise Identity administrator console.

Other BBM Enterprise features

Timed automatic message deletion and message retraction also minimize the risk of unauthorized data access.

Device management

As discussed in section 2.2.2 *HIPAA program covers an entire system of policies, procedures, and processes*, an organization should institute safeguards for device use and management to ensure its entire system is HIPAA compliant. Many of these safeguards are supported by other BlackBerry products such as BlackBerry UEM.

BBM Enterprise contributions to HIPAA compliance

The following table summarizes the best practices for implementing the specifications of the HIPAA technical safeguards and how the BBM Enterprise solution contributes to compliance.

Table 3. BBM Enterprise contributions to HIPAA compliance

HIPAA technical safeguards			
Standard	**Implementation specification**	**Best practices for implementation**	**BlackBerry feature or system component *each described above)**
A. Access controls	Unique user identification	Authentication Services	Unique encryption key
A. Access controls	Emergency access procedure	-	Device Management
A. Access controls	Automatic logoff	Configurable Idle Timeout	Device Management
A. Access controls	Encryption and decryption	Advanced Encryption Standard (AES)	End-to-end encryption protocol
B. Audit Controls	Record and examine activity	Monitoring	BlackBerry Audit & Archiving Service
-	-	Logging and Alerting	BlackBerry Audit & Archiving Service
C. Integrity	Mechanism to authenticate ePHI	Unique Session Keys	BlackBerry message integrity and authentication Unique encryption key
C. Integrity	Integrity controls	Advanced Encryption Standard (AES)	End-to-end encryption protocol
-	-	Authentication services	BlackBerry message integrity and authentication
-	-	Unique Session Keys	BlackBerry message integrity and authentication Unique encryption key
D. Person or Entity Authentication	Unique user identification	Authentication services	BlackBerry message integrity and authentication Unique encryption key
E. Transmission Security	Encryption and decryption	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 integrity and authentication
-	-	Unique Session Keys	Unique encryption key

Conclusion

Your mobile strategy requires an end-to-end solution for transmitting, managing, and storing in compliance with HIPAA—the overall security and compliance of your complete system depends on the strength of each component. BBM Enterprise provides a proven, standards-based pipeline for real-time ePHI messaging, which can serve as the trusted centerpiece of your solution.

This appendix lists the acronyms that are used in this document:

Acronym	Full term
AES	Advanced Encryption Standard
BAAS	BlackBerry Audit & Archiving Service
CTR	Counter
DH	Diffie-Hellman
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EC-SPEKE	Elliptic Curve – Simple Password Exponential Key Exchange
ePHI	Electronic Protected Health Information
FIPS	Federal Information Processing Standards
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HMAC	Hash-based Message Authentication Code
KDF	Key derivation function
NIST	National Institute of Standards and Technology
PGP	Pretty Good Privacy
SHA	Secure Hash Algorithm
SRTP	Secure Real-time Transport Protocol
TLS	Transport Layer Security