ENABLING MOBILE USERS AND STAYING COMPLIANT

How Healthcare Organizations Manage Both

Whitepaper
Enabling Mobile Users and Staying Compliant: How Healthcare Organizations Manage Both

Operating in a regulated industry, like healthcare, adds a layer of complexity to many things – including mobility.

While enterprises in other industries may be concerned about security – health-related organizations and their business associates are obliged by law to conform to detailed rules around storing and sharing sensitive data.

In the U.S., conforming got a little tougher in the fall of 2013, when changes to the Health Insurance Portability and Accountability Act (HIPAA) were implemented. These updates enhance a patient’s privacy protections, provide individuals with new rights to their health information, and strengthen the government’s ability to enforce the law. In particular, they “expand many of the requirements to business associates of these entities that receive protected health information, such as contractors and subcontractors. Some of the largest breaches reported to the Department of Health and Human Services (HHS) have involved business associates.”
Penalties for noncompliance are stiff, topping out at $1.5 million per violation. In the last 3 years, there have been over 70,000 HIPAA violation complaints.²

These new rules add to an already complex governance structure, as healthcare workers store and share more and more sensitive information on mobile devices. Those devices are often now BYOD (Bring Your Own Device) – smartphones and tablets staff own personally and bring for use at work. While some accounts suggest BYOD has widely penetrated the healthcare world, the reality is that what users can do with those devices at work varies greatly. And that’s because healthcare providers are struggling to enable collaboration and efficient workflows yet still comply with regulations.

It’s a tricky balance. On one hand, management understands that information must flow between the physicians and administrative staff it needs to reach. On the other, they’re well aware of the fact that, handled inadequately, these simple exchanges may result in million-dollar fines.

According to one industry insider, “Most hospitals are grossly noncompliant. All clinical staff and most administrative staff are just doing what they can to get things done… sharing information and not having any sort of an audit trail is really problematic. That is a HITECH violation and a HIPAA violation.” He adds that some hospitals are putting the liability on employees if they share data externally, with warnings that pop up before they send email attachments or share files – some even requiring the sender to click on a box saying they accept the risks.³

A High-Profile HIPAA Violation

In August 2014, the BBC reported that a major US healthcare conglomerate sustained a cyber-attack resulting in the “theft of 4.5 million people’s personal data.”⁴

Analysts speculate that the attack on Community Health Systems originated in China. Stolen details included patient names, addresses, birthdates, telephone numbers and social security numbers.

Experts warned that the data could be used to steal people’s identity. And for the company, the breach could cost as much as $150 million.⁵

Among those projected costs: hefty fines for violations of HIPAA privacy laws. And HIPAA enforcers are in crackdown mode.

The BBC report cites Lamar Bailey, director of security research and development at cybersecurity firm Tripwire, who said “when personal information is stolen – name, address, phone number, birthdates, and social security number – it impacts the person and not a company.” He added: “This is the information needed for identity theft to allow criminals to open accounts in the names of the 4.5 million victims.”
Enabling Mobile Users and Staying Compliant: How Healthcare Organizations Manage Both

How HIPAA’s chief enforcer sees it: “In many respects, HIPAA compliance and enforcement is a lot like high school math. It’s all about showing your work. It’s all about showing you have comprehensive policies and procedures in place and are treating it as an ongoing, living process. Compliance is continual, not done once and set aside when inconvenient. The world is not perfect, and breaches are still going to happen. What we’re going to look at is, have you done everything you reasonably can do to prevent breaches?”

- Leon Rodriguez, Director, Office for Civil Rights, U.S. Department of Health and Human Services

Government bodies provide a number of resources to help healthcare organizations get and stay compliant with HIPAA requirements. But it’s still an incredibly complex and time-consuming task, and one that carries on indefinitely, as new legislation emerges, and new technology enters the workplace.

Compliance will always be a human challenge — but there are technical solutions designed specifically to help regulated industries tackle the issues.

What the government tells healthcare providers

The U.S. Department of Health and Human Services provides guidance for healthcare organizations, like the recommendations below, but many still struggle to interpret the rules and put them into action.

1. Decide
Decide whether mobile devices will be used to access, receive, transmit, or store patients’ health information or used as part of your organization’s internal networks or systems (e.g. your EHR system).

2. Assess
Consider how mobile devices affect the risks (threats and vulnerabilities) to the health information your organization holds.

3. Identify
Identify your organization’s mobile device risk management strategy, including privacy and security safeguards.

4. Develop, Document, and Implement
Develop, document, and implement the organization’s mobile device policies and procedures to safeguard health information.

5. Train
Conduct mobile device privacy and security awareness and training for providers and professionals.
How BlackBerry supports healthcare compliance

Gold Level EMM: Specifically designed for high-security organizations and users

Securing the device
Let’s start with the end user and work our way back. As we’ve seen, BYOD has made its mark on healthcare. Staff are using their own devices for a range of activities from simple internet access to using applications to update health records on the fly.

BYOD in healthcare isn’t going away. For users on iOS and Android™ devices, BlackBerry® offers Secure Work Space, a containerization, application-wrapping and secure connectivity option that brings healthcare organizations a higher level of control and security.

› Users get convenient, unobtrusive, secure access to corporate email, calendar, contacts, notes and tasks through a single application.
› They can access a secure Work Browser, so they can safely browse internal pages (intranet) and web pages from right within the Secure Work Space.
› They can tap into Documents To Go® to create, view and edit work documents, with the formatting and features they’re used to on their desktop computers.
› Approved apps that medical staff need for work are accessible in the Secure Work Space, too.
› Outside the Secure Work Space, healthcare workers can carry on using the device for their personal lives, knowing their work data is kept separate and secure.

Sounding alarm bells
The FBI and other agencies have been sounding alarm bells for some time now. In April of 2014, they issued a private notice to healthcare providers, which made the point clear:

“The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.”

Health data is “far more valuable to hackers on the black market than credit card numbers” because it often includes details that can be used to tap into bank accounts or “obtain prescriptions for controlled substances,” wrote Reuters’ Jim Finkle at the time.

And while the healthcare industry can be slow to make changes, cybercriminals are on the cutting edge, getting better at what they do every day, and getting bolder too.¹⁷

Some users and use cases require the ultimate security. BlackBerry® 10 devices enable it.

With BlackBerry® Balance™ technology, on BlackBerry 10 devices, personal and work apps and information are kept separate, from the operating system on up. The Work Space is fully encrypted and secured, so IT can protect all sensitive content and applications, while users get the most out of their smartphone for their personal use.

Gartner calls BlackBerry Balance “the best example of the separation of corporate data from personal data while retaining a strong user experience.”⁸

› Data Leak Prevention (DLP) is built right in, so users can’t accidentally copy and paste work data into personal channels, like social media apps.
› The apps staff need can be pushed right to the work space on their smartphone or made available through a corporate app storefront.
› Still, organizations have the option to deploy a corporate-only use model where device features and capabilities, including social media feeds and public application access, can be turned off.
Protecting data in transit
BES12 manages BlackBerry, iOS, Android, and Windows® Phone devices.

The proven BlackBerry security model gives healthcare providers ‘always-on’, AES-encrypted access to systems behind the firewall, through a single outbound port, so they don’t have to worry about people stealing data out of the air.9

Managing it all: BES12
BES12 is the command and control center for the secured healthcare organization. BES12 lets healthcare IT teams manage mobility permissions, policies and protection, by individuals and by groups, across endpoints, apps, activities and critical data. With BES12, users connect confidently and securely – and only as authorized – to approved enterprise apps, business partners and cloud providers.

Using encryption, containerization, app-wrapping and BlackBerry’s secure global infrastructure, BES12 locks down critical data both on-device and in-transit. All mobile management traffic passes through a single port behind your firewall, 3101, via our world-renowned NOC, to ensure user privacy and data security. With secured work spaces on iOS, Android and BlackBerry devices, your data traffic is also routed through a consolidated port, protecting your most important asset – your data. BES12 is built on proven security you can trust.

Backed by industry leading global support services, BES12 offers a seamless, scalable and cost effective way for you to truly mobilize your business.

Reporting and monitoring – critical for compliance
With BlackBerry reporting capabilities, IT administrators in healthcare have immediate access to a unified dashboard of key metrics across their entire mobile deployment, and can drill down into more detail to take immediate action, or export data for further analysis.

These areas include:
› Device activations
› Device last contact time
› Device compliance state
› Devices by platform
› Devices by carriers
› Top five applications deployed
› Top five mobile devices

Multiple components to manage and multiple potential points of failure
Integrated security with BlackBerry: Complete control. One partner.
And, alongside BES12, BlackBerry has launched new solutions for enterprise productivity that can help your healthcare organization do more every day, and do it securely. Among them:

**BBM™ Protected**

Designed for regulated environments like healthcare organizations, BBM Protected offers an enhanced security model for BBM messages sent between BlackBerry smartphones that protects corporate data in-transit by adding an additional layer of encryption to BBM. BBM Protected allows employees to take advantage of the speed, reliability and privacy of BBM for faster communication, collaboration and decision making while providing enhanced security over corporate data.

**Enterprise Identity by BlackBerry®**

Make it easy for employees to experience the benefits of cloud-based applications from any device with a browser using a single set of credentials. For IT, Enterprise Identity by BlackBerry simplifies the management of cloud-based applications with a single point of entitlement, control, and audit for all cloud apps.

**VPN Authentication by BlackBerry®**

Stop depending on outdated one-time password (OTP) tokens that result in another device for employees to carry and another password to remember. With VPN Authentication by BlackBerry, your employees’ iOS, Android or BlackBerry devices replace your expensive OTP hardware solution with Public Key Infrastructure (PKI) based two-factor security that helps reduce overall costs.

Find out more about these and other services at [www.blackberry.com/enterprise](http://www.blackberry.com/enterprise)
Enabling Mobile Users and Staying Compliant: How Healthcare Organizations Manage Both

To find out more and to sign up for a free 60-day BES12 trial, head to blackberry.com/enterprise

1 Available at: http://www.hhs.gov/news/press/2013pres/01/20130117b.html
2 Available at: resource.onlinetech.com/hipaa-in-a-hitech-world-hipaa-violations-on-the-rise-according-to-director-of-ocr/
4 Available at: http://www.bbc.com/news/technology-28838661
5 Available at: http://www.healthit.gov/providers-professionals/five-steps-organizations-can-take-manage-mobile-devices-used-health-care-pro
6 Available at: http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423
7 Available at: http://ca.blackberry.com/campaigns/gartner-magic-quadrant-mdm.html
8 Single outbound port/VPN-less secure connectivity is available for BlackBerry OS devices when managed through BES5 and for BlackBerry 10 devices when managed through BES12. For iOS and Android devices, secure connectivity is enabled in the Secure Work Space with Gold level EMM.
9 60-day Free Trial Offer: Limited time offer; subject to change. Limit 1 per customer. Trial starts upon activation and is limited to 50 Gold BlackBerry subscriptions and 50 Secure Work Space for iOS and Android subscriptions. Following trial, customer must purchase subscriptions to continue use of product. Not available in all countries. Subscriptions can be purchased direct or from authorized resellers. When a system is upgraded to production, the trial subscriptions will no longer be available. This Offer is void where prohibited and is subject to modification, extension or early termination at BlackBerry’s sole discretion.

© 2014 BlackBerry. All rights reserved. BlackBerry®, BBM™ and related trademarks, names and logos are the property of BlackBerry Limited and are registered and/or used in the U.S. and countries around the world. All other trademarks are the property of their respective owners.