



Enabling Mobile Users and Staying Compliant

**How Healthcare
Organizations Manage Both**

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."¹

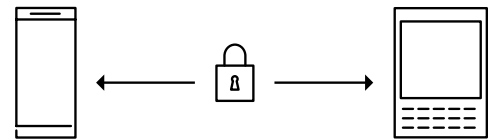


Penalties for noncompliance are stiff, topping out at \$1.5 million per violation. In the last 3 years, there have been over 70,000 HIPAA violation complaints.²

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 that 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 non-compliant. 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 identities. 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."

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 your 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.⁶

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.⁷

Mobile Productivity Meets Certified Security

BlackBerry Enterprise Mobility Suite

Secure productivity

BYOD has made its mark on healthcare, and it isn’t going away. 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.

The BlackBerry® Enterprise Mobility Suite offers the industry-leading Unified Endpoint Management (UEM) solution to meet critical healthcare needs, with a comprehensive app ecosystem to provide your organization more value, more innovation and more security than ever before.

Users can access the apps and content they need, where and when they need it. Meanwhile, IT stays in complete control of the entire fleet.

- Users get VPN-less access to intranet and web apps from any device.
- They get convenient and secure access to work-related tools — like email, calendars, contacts and documents — that integrate for a seamless work experience.
- Critical Microsoft® and third-party apps are completely controlled, so medical staff have secure access to the tools they need anytime.

- IT can unlock new opportunities for productivity, with the ability to develop and manage custom apps for your organization.
- Establish who has permission to view, edit, print and share organizational content, and keep all files secure — even when they’re shared outside the organization.

Securely contained

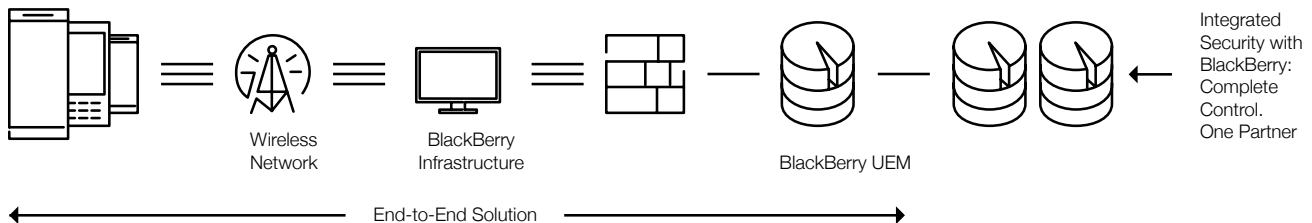
With the BlackBerry Enterprise Mobility Suite, personal and work apps and information are kept separate. Organizational data is fully encrypted and secured, so IT can protect all sensitive content and applications, while users get the most out of their devices for personal use.

- 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.
- Push the apps staff need right to their devices, or make them available through a corporate app storefront.
- Where necessary, organizations have the option to deploy a corporate-only use model, where device features and capabilities, including social media feeds and public app access, can be turned off.

Backed by industry-leading global support services, the BlackBerry Enterprise Mobility Suite offers a scalable way to truly mobilize your organization, and navigate the ever-changing mobility landscape in the future.

Protecting data in transit

BlackBerry® Unified Endpoint Manager (UEM) manages iOS®, Android™, Android™ for Work, Samsung Knox™, Windows®, macOS and BlackBerry® devices. The proven BlackBerry security model gives healthcare providers ‘always-on’, AES-encrypted access to systems behind the firewall, so they don’t have to worry about people stealing data out of the air.



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.

Managing it all: BlackBerry UEM

BlackBerry UEM is at the heart of the BlackBerry Enterprise Mobility Suite, acting as a command and control center for the secured healthcare organization. BlackBerry UEM lets healthcare IT teams manage mobility permissions, policies and protection, by individuals and by groups, across endpoints, apps, activities and critical data. Users connect confidently and securely — and only as authorized — to approved enterprise apps, business partners and cloud providers.

Using encryption, containerization and BlackBerry’s secure global infrastructure, BlackBerry UEM locks down critical data both on-device and in-transit. All mobile management traffic passes through a single port behind your firewall, via our world-renowned NOC, to ensure user privacy and data security.

BlackBerry UEM is built on proven security you can trust.

BlackBerry provides additional solutions for enterprise productivity that can help your healthcare organization do more every day, and do it securely. Among them:

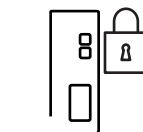


BBM Enterprise

BBM® Enterprise is a truly mobile, cross-platform messaging and collaboration tool that runs on employees' chosen devices — including iOS, Android and BlackBerry devices. It provides the same user-friendly experience that's earned BBM® millions of fans worldwide — with the end-to-end security enterprise needs.

One-to-one chats, group discussions, video communications and file sharing all happen with the protection required by security-conscious and regulated organizations — and all with an immediacy and accountability that's hard to achieve through any other communication channel.

BBM Enterprise uses a FIPS 140-2 validated cryptographic library and leverages BlackBerry's secure infrastructure to protect data while it's in transit and at rest.



BlackBerry Enterprise Identity

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, BlackBerry® Enterprise Identity™ simplifies the management of cloud-based applications with a single point of entitlement, control, and audit for all cloud apps.



BlackBerry 2FA

Stop depending on outdated one-time password (OTP) tokens that result in another device for employees to carry and another password to remember. With BlackBerry® 2FA™, your employees' iOS, Android and BlackBerry devices replace your expensive OTP hardware solution with Public Key Infrastructure (PKI) based two-factor security that helps reduce overall costs.



AtHoc

Communicate and collaborate securely during times of crisis. The AtHoc™ Networked Crisis Communication Platform empowers you to alert the people you care about with a unified message, and account for them throughout an event. You can also connect with external organizations, so that the community can respond to a crisis together.

Find out more about these and other services at blackberry.com/enterprise

The BlackBerry Enterprise Mobility Suite has something to offer at every stage of the mobility lifecycle. Visit blackberry.com/suite to learn more.

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/

³ Available at: blogs.wsj.com/riskandcompliance/2013/09/26/hospitals-allowing-byod-face-complications-with-new-hipaa-rule/

⁴ Available at: www.bbc.com/news/technology-28838661

⁵ Available at: www.forbes.com/sites/danmunro/2014/08/24/assessing-the-financial-impact-of-4-5-million-stolen-health-records/

⁶ Available at: www.healthit.gov/providers-professionals/five-steps-organizations-can-take-manage-mobile-devices-used-health-care-pro

⁷ Available at: www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423