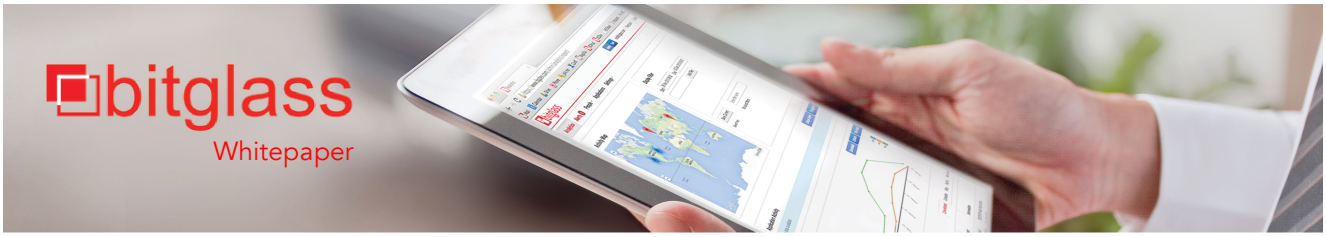

HIPAA Compliance, PHI and BYOD

Healthcare providers are responsible for securing data on endpoint devices, and for ensuring compliance with HIPAA regulations. This becomes even more challenging when BYOD is introduced into the environment. Healthcare practitioners are as passionate about their mobile devices as anybody, and 90% of them use their personal smartphones for work. On the surface, this makes a lot of sense – not only is the practitioner already familiar with the device, but BYOD can also help cut costs. The problem? Securing a personally owned device is much harder than securing a managed device. When Protected Health Information (PHI) is accessed from these devices, how can you comply with strict HIPAA requirements? Any BYOD program put into place must balance PHI protection and data security with flexibility and mobility for the organization's staff.

When they get the latest and greatest gadget, your staff isn't necessarily going to bring it to IT to have it configured and locked down. Even if they do, they won't like signing over control of their personal devices to IT. And if a doctor has affiliations with multiple providers, existing solutions, such as MDM are out of the question. The appropriate approach is one that secures your organization's data (including PHI), without taking control over their personal device or data, and without conflicting with other security software.

Limitations of Incumbent Solutions

The most common approach to addressing BYOD security is to manage employee-owned devices with "Mobile Device Management" or "Mobile Application Management" solutions. With such solutions, each employee is required to have a software agent installed on his or her mobile device, ceding control of the device to the organization. The software agent on the device controls how the practitioner uses the device, which applications may be installed, and tracks the employee's geographic location etc. If the staff member leaves the organization, IT may completely wipe any and all data on the user's device, including both personal and corporate applications and data. These solutions are difficult to deploy and maintain, requiring the installation of software on mobile devices that are often not owned by the provider. Furthermore, such solutions invade employee privacy since they gain access to all personal

applications and data on the smartphone. While IT has more control, many employees, including CIOs and IT managers, dislike the solution.

Furthermore, MDM solutions have limited applicability in uses cases involving practitioners with multiple affiliations. Many doctors and care providers have multiple affiliations and email accounts associated with each affiliation. For example, a doctor may work at two different hospitals, and have email accounts at both hospitals. It is technically impossible for the doctor to install two different MDM agents on her smartphone, ceding control of the phone to both hospitals at the same time.

HIPAA requires that PHI such as medical record numbers, names, social security numbers etc. not be downloaded to BYOD. Such blocking capabilities are broadly referred to as "data leakage prevention" and MDM/MAM solutions have no such functionality.

Characteristics of a BYOD Security Solution for Healthcare

A fresh approach to security is required to secure corporate data in BYOD deployments. Such a solution must offer a frictionless experience for employees (even those with multiple affiliations) while providing IT with data security and visibility, enabling the organization to embrace BYOD while remaining compliant. The following sections outline the requirements for a solution that addresses all of these areas.

IT - Data Security and HIPAA Compliance

IT must be able to block and control critical information before it is downloaded to devices by a set of rules that syntactically and contextually recognize PHI. The security solution must dynamically detect and redact PHI as data flows to BYOD clients in order to maintain HIPAA compliance.

Furthermore, if a staff member leaves the organization, IT needs to be able to selectively wipe corporate data, without disturbing personal data or data from any other account on the device. This process should be straightforward for IT departments with minimal administrative overhead.

IT - Visibility and Control

With sensitive data moving onto BYOD, IT needs visibility and control. Visibility should be comprehensive, providing insight into all user activity across all mobile devices in an organization. Regulatory compliance requires detailed audit logs including user information, location, IP address, type of device, URL accessed and any other available parameters. When a device is lost or misplaced, IT should be able to produce a list of all data on the device to evaluate the risk associated with the loss. From a security standpoint, an ideal solution should

provide actionable insights and alerts into suspicious behaviors and activities. The solution should provide the ability to restrict these types of activities via rich, contextual access controls that allow the enterprise to decide who gets access to what, and under what conditions.

IT also needs visibility into what happens with sensitive corporate data after it has been downloaded to employee devices. Specifically, IT needs to know where data travels, and the sensitivity of that data. Did it originate from certain users or applications? Does it match keywords or patterns of known sensitive data? Visibility—transaction logging, alerts and more—deters unauthorized dissemination of information outside of the organization and helps to find offending employees before damage has been done.

IT - Easy to Deploy

Every IT organization is short on resources, and one of the biggest advantages of BYOD is that they help lighten the IT burden of management and operations. Likewise, security solutions must be cloud-based, deploy quickly and easily with minimal administrative overhead, and scale easily. Data should be secured for BYOD without installing software agents on personally owned devices, ensuring employee privacy and avoiding conflict with other "device management" solutions.

Employees - Easy to Use

Today's practitioners are as busy as ever, and minutes can be the difference between life and death. Consumer mobile technologies are high quality and high-performance. Doctors, nurses, and other staff expect IT to offer solutions that are comparable. Security solutions that slow people down introduce risk, lower productivity and encourage employees to adopt workarounds that defeat security policies. For example, employees prefer familiar native email applications on their mobile devices for personal and work use. An MDM solution might force an unfamiliar third-party email client for work use, hampering the user.

Employees - Ensuring Privacy & Trust

Employees expect privacy in their personal communications. Security solutions that transport, handle or inspect private user communications are viewed with great suspicion by employees and hinder productivity. For example, an MDM solution installs software on employee-owned mobile devices controlling what they can and cannot do with their device. As a second example, a forward proxy security solution routes and inspects all traffic, including employee's personal communications and Google searches. Ultimately, employees have the expectation and the right to privacy. Security solutions that invade privacy drive employees to workarounds that circumvent IT security policies.

Data Security & HIPAA Compliance with BYOD

In summary, enabling BYOD offers great productivity gains for the modern healthcare organization, but risks data security and HIPAA compliance. Despite these risks, 90% of healthcare employees use their personal devices for work purposes. To restore security and compliance, choose a security solution that simultaneously satisfies two constituencies: the IT department seeking security and control, and employees seeking usability and privacy. To learn more, contact Bitglass (www.bitglass.com) for a free demonstration.

www.bitglass.com
Phone: (408) 337-0190 - Email: info@bitglass.com

bitglass

About Bitglass

As enterprises adopt BYOD and cloud applications, IT is faced with securing corporate data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are simply not suited to solving this task, as they were developed to secure the corporate network perimeter. Adding to the challenge, employees have an expectation of privacy when using the same mobile devices and apps for work and personal use. Bitglass brings to market breakthrough technologies that deliver the security and visibility IT needs to enable mobile and cloud in the workplace, while respecting user privacy. Bitglass was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution. We are based in Silicon Valley and we are backed by Tier 1 investors, Norwest Venture Partners and NEA, via a $10M investment in February 2013. Find us at www.bitglass.com or info@bitglass.com.

www.bitglass.com
Phone: (408) 337-0190 - Email: info@bitglass.com

bitglass