



BYOD, Secure
Messaging and
HIPAA Compliance

Did you know?

- According to [Spyglass](#) research, nine in 10 hospitals have already made or are making significant investments in smartphones and secure unified communications.
- 91 percent of healthcare IT leaders said they would benefit from an enterprise-wide mobile device initiative, as per a recent JAMF survey.





Reflection

- These research takeaways present a strong viewpoint on how healthcare is embracing digital transformation and disruption with open arms. The survey response is a clear indicator of what the future holds for clinical communications. Mobile will play a major role in streamlining communications for patient care teams, paving its way for clinical transformation. But this massive technology comes with a cost if risks are not mitigated well. The big question that needs further investigation is how does one create a fool-proof secure environment around clinical communication applications on mobile devices, especially in times where bring your own device (BYOD) is becoming ubiquitous and the pager technology is not holding up to robust two-way communication standards.
- A strong response and solution to these multitude of concerns can be constructed by allowing hospital employees to embrace BYOD policies, where they would bring their personal smartphones to work. While this option also has security concerns wrapped up in it, BYOD will enable hospitals to bring on the benefits of secure hospital messaging and ensure HIPAA compliance.



Introduction

This eBook will explore the benefits of BYOD. At the same time, it will investigate how chief information officers (CIOs) can manage potential risks they might face from BYOD and how to ensure an effective mobile solution for their organization's future.

This eBook will examine the following points:

- BYOD challenges
- BYOD – Managing Risk
- How BYOD can improve hospital secure messaging and HIPAA compliance

Challenges to BYOD – What’s the pushback?

In the past, healthcare organizations have paid dearly due to breaches. A case in point is the Children’s Medical Center of Dallas who paid \$3.2 million to HHS over patient privacy breaches linked to an unencrypted, non-password protected BlackBerry device.

HIPAA

HIPAA is often held up as further reason for not bringing BYOD onboard. HIPAA concerns should be foremost when using just about any electronic device in healthcare, since HIPAA violations can be expensive.

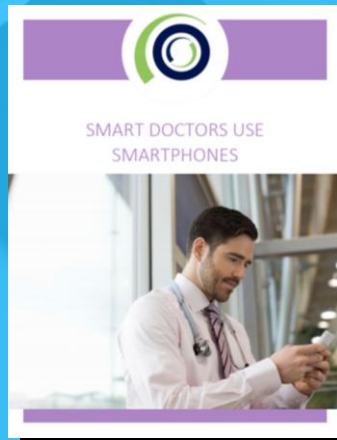
When faced with the possibility of implementing smartphone technology, institutions believe that HIPAA compliance is unmanageable. A doctor might even snap a quick photo of a curious rash or wound to share with a colleague or specialist, then have that photo saved in a queue alongside family photos. While this is a clear HIPAA violation, there is not much that institutions can do to manage these exchanges.

Cost

Budgets also play a significant role in executives’ thinking. Fifty-six percent of surveyed CIOs said they see budget and resource constraints as the biggest risk in keeping data safe. CIOs worry that even with a BYOD cost savings, they wouldn’t necessarily have the funds to manage the security of smartphone devices. Indeed, even when security measures are installed, many doctors and nurses simply design work-arounds that bypass safety and security protocols in defiance of HIPAA standards.

Security

Indeed, security is the fear that wags the dog from efforts to lead innovation. CIOs worry that by enabling further BYOD use, they will expose their institutions to unknown risks. And this fear is not unreasonable as a significant source of intrusions are from lost or stolen devices. Companies that have implemented BYOD often struggle to protect against data loss and ensure that communications remain secure.

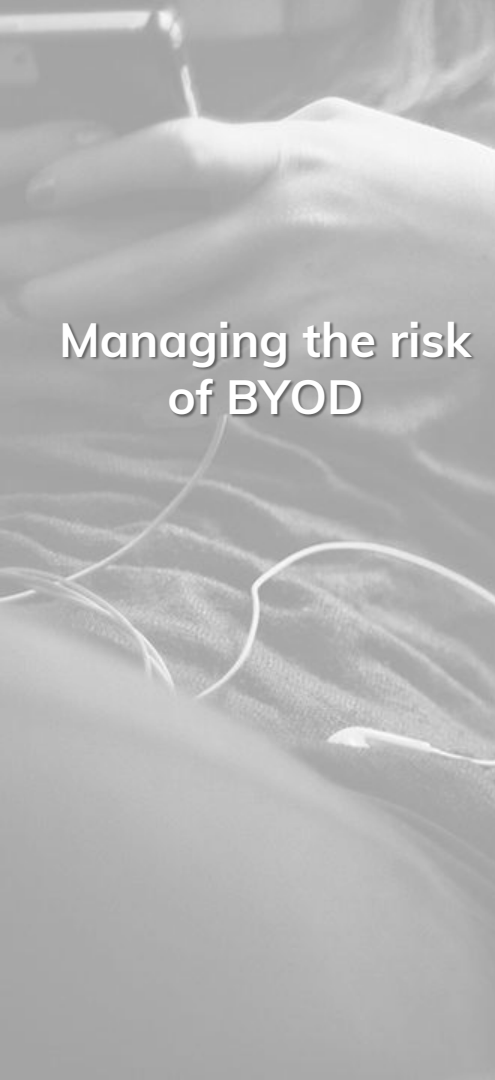


Smart Doctors Use Smartphones

Ever wondered why doctors have made the switch from pagers to smartphones? Download our guide to learn more!

SKIP






Managing the risk of BYOD

An important part of effective BYOD management is handling the potential risks that come from actual BYOD use. When hospital employees are beneficiaries of a BYOD policy, they can download messaging applications. These applications should be subjected to high evaluation standards to ensure that they stand through the test of data breach attempts.

Furthermore, policies should be put in place to ensure smartphones are password protected, that applications have end-to-end security and that remote wipe is made available on any messaging application.

Moreover, the applications team members download need to provide:

- A secure sign-on process: Password enable access to the smartphone as well as access to the application
- Encrypted messaging: Messages should be encrypted both at rest and in transit
- Incorporate delivery and read receipts: Make sure that messages come with an audit trail so receipt can be ensured. This ensures the intended path of the message has been followed.
- Have date and time stamps: Date and time stamps provide further evidence of who saw the message and when.
- Customizable message retention time frames: Enable retention of messages for a reasonable time after they are sent to ensure proper record keeping for unexpected investigations.
- Have a specified contact list for individuals authorized to receive and record orders: Only individuals who are authorized to receive messages should be included in the contact list. This ensures that sensitive patient information is not accidentally shared with unauthorized individuals.



BYOD's importance for ensuring secure communications and HIPAA compliance

By using applications like OnPage, healthcare institutions can overcome the risks BYOD can pose and see significant benefits to their overall institution. These benefits include:

Improved Security: As discussed previously, using secure messaging applications ensure that the communications are encrypted with end-to-end security. This eliminates the opportunity for messages to be intercepted by malicious parties. Patient confidentiality as well as patient privacy is maintained.

Cost Management: With BYOD, hospitals don't pay for the hardware as it is already in the employee's possession. The hospital only pays for the secure messaging application. Furthermore, if the CIOs adopt the correct messaging application then the security concerns noted above will already be addressed.

HIPAA Compliance: By choosing the right secure messaging solution, CIOs can ensure that messages adhere to HIPAA regulations and help protect the clinic or hospital from HIPAA violations.

Improved Patient Outcomes: The use of mobile technology can be correlated to increased patient satisfaction, stemming from improved clinical communications and collaboration. According to a recent University of Pennsylvania study, the use of smartphone secure messaging led to an earlier release of patients as compared to the control group. According to the study, patients whose providers used mobile secure text messaging left the hospital about 0.77 days sooner, equivalent to about a 14 percent reduction in their overall hospital stay.



OnPage's award-winning, HIPAA-compliant incident alert management and clinical communications system for healthcare professionals provides the industry's only ALERT-UNTIL-READ notification capabilities, ensuring that critical messages are never missed. Through its platform and smartphone app, OnPage helps streamline workflows and improve patient outcomes.

OnPage's escalation, redundancy and scheduling features make the system infinitely more reliable and secure than pagers, emails, text messages and phone calls. OnPage shrinks resolution time by automating the notification process, reducing human errors and prioritizing critical messages to ensure fast response.

Whether to minimize IT infrastructure downtime or to reduce the response time of healthcare providers in life-and-death situations, organizations trust OnPage for all their secure, HIPAA-compliant, critical notification needs.

Thanks!

A grayscale background image showing a hand holding a piece of white chalk, writing on a chalkboard. The word 'Konm' is partially visible on the board.

Any questions?

CALL US!

Phone +1 (781) 916-0040

[Or schedule a demo!](#)

THANK YOU!