ONPAGE | GUIDE

Questions to Ask Before Adopting Secure Messaging

OnPage Corporation Tel: 781-916-0040 www.onpage.com

It is the responsibility of healthcare administrators to move away from legacy technologies and start propagating the use of a clinical communications solution, ensuring that healthcare practitioners understand a pager solution's relative advantage over unreliable, antiquated pagers.

Eighty percent of hospitals still use pagers for clinical communications and internal messaging[i]. But, why are they still being used? Organizational dependence on legacy, communication systems can be attributed to three factors, including:

1 – Perceived Costs

Although more cost-effective than traditional paging systems, some hospitals are reluctant to trade their pagers for a more secure, clinical communications solution. That is because some healthcare administrators perceive pager replacement options to be more costly than traditional pagers.

But, that assumption is far from the truth. For instance, a simple, ordinary Motorola pager can cost a healthcare organization nearly $230 per year, per user[ii]. Also, healthcare organizations in the U.S. are expected to pay an additional, monthly charge of $20 for nationwide coverage[iii].

Even worse, healthcare facilities that use pagers are highly susceptible to costly protected health information (PHI) or data breaches. Hospitals that have experienced data breaches have been fined an average of $313,000 for confiscated, sensitive patient information[iv].

Additionally, pager replacement options help healthcare organizations save 60 percent in costs over traditional, paging devices. Not only do organizations save in costs, but they can also benefit from global coverage—in over 175 countries—when using a secure, pager replacement solution[v].

Healthcare organizations should stop asking themselves whether or not a secure, clinical communications alternative is (1) more expensive than pagers or (2) worth its perceived cost. In its place, organizational change agents should ask themselves when they can finally start implementing a more secure and cost-effective pager replacement solution.

2 – Resistance to Change

It is common for hospital faculty (i.e., doctors and nurses), as well as personnel in most industries, to resist the widespread propagation of new technology within their organizations.

Resistance to new technology adoption is based on:

- Faculty comfort and familiarity with legacy technologies
- The unfamiliarity with pager alternatives and their reliability
- A perceived, complicated and lengthy onboarding process that disrupts care team operations and workflows

Heavy resistance to change can be resolved by communicating a pager solution's relative advantage (i.e., the benefits of pager replacement solutions over subpar substitutes or in this case, pagers). For instance, change agents can tout that pager replacement solutions (1) promote quicker patient care for greater, patient satisfaction (2) improve their facility's bottom line (3) streamline the check-in process and (4) foster care team collaboration and employee morale[vi]. Also, most caregivers nowadays would prefer to carry just one communication device –their smartphones.

3 – Security Concerns and HIPAA

In the healthcare industry, it is key that organizations protect sensitive patient information and avoid hefty costs attributed to a possible data breach.

However, hospitals continue to rely on pagers for HIPAA compliance, as they believe that smartphone-based alternatives equate to breaches caused by personal, mobile device use. Simply put, some administrators are under the impression that mobile, pager solutions enable physicians to carelessly use their phones, causing PHI breaches in the process.

However, this is a false assumption. Clinical communication solutions provide SSL encrypted messaging with remote-wipe capabilities. By adopting such a platform, healthcare organizations can better safeguard patient information, even when a physician's phone is intercepted by malicious parties. It is a sound way to ensure that hospitals meet HIPAA requirements.

The Goal of This Guide

Understanding that pager replacement solutions are more beneficial and secure for healthcare organizations is an important first step when diverging away from pagers.

This guide outlines a set of questions that healthcare change agents should ask when considering pager solutions. Additionally, this guide will help healthcare professionals understand whether or not a considered pager alternative meets important, organizational requirements.

Question One: Does the Alternative You Are Considering Actually Update Pager Technology?

Before answering the question, it is important to understand the limitations and problems with pagers. Pager limitations—in terms of communication workflow—include, but are not limited to:

- Messages being easily intercepted by unauthorized third parties[vii]
- Providing only the receipt of messages—most pagers do not let physicians or nurses respond to messages on the pager
- Their dependence on an aging infrastructure[viii]
- Causing delays due to one-way and numeric messaging[ix]

Moving away from inefficient pagers is an important task for healthcare organizations. When selecting a pager replacement solution, change agents need to make sure that the considered technology provides encrypted, two-way communication and is able to efficiently integrate with existing, hospital workflows.

Additionally, organizations need to determine whether or not a technology under consideration requires a significant financial outlay on the part of the hospital or treatment center. Facilities should also determine whether or not a considered technology aligns and works well with existing technologies such as personal, smartphone devices. As over 85 percent of healthcare employees bring their own devices to work already, integration with smartphones is a way for facilities to control costs[x].

Question Two: Is the Solution HIPAA Compliant?

The goal of HIPAA-compliant technology is to protect the privacy of individuals' health information, while allowing entities (i.e., hospitals) to adopt new technologies that improve the quality and efficiency of patient care.

HIPAA compliance must be a key component of any secure messaging alternative that a facility considers and investigates.

Hospitals need to ensure that a pager alternative provides encrypted, HIPAA-compliant communications for both "at rest" and "in transit" messages, preventing sensitive information from being intercepted or improperly read. Additionally, a paging solution must provide a sign-in process for authorized users per device. In this way, malicious parties or unauthorized users are unable to access sensitive, clinical information (e.g., patient information and records).

Question Three: Does the Technology Ensure Persistent Alerting to Guarantee the Recipient Does Not Miss the Alert?

In life or death situations, it is critical that physicians receive timely notifications to provide appropriate care for patients. Additionally, it is common that healthcare practitioners miss alerts through their antiquated pagers when outside hospital grounds.

When choosing a more reliable, pager replacement solution, institutions must ensure that the technology provides persistent notifications that keep sounding until the alert is acknowledged, and are equipped with distinguishable, audible alarms to differentiate them from other notifications.

Furthermore, the technology must provide support for on-call rotations and escalation policies that can be predetermined through a comprehensive, web-based console. In this way, qualified physicians will always receive alerts based on customizable, digital schedules. In the case that a critical alert is missed by an intended physician in a given amount of time, it is then escalated to the next healthcare practitioner in line.

Question Four: Does the Technology Provide Delivery Confirmation?

The technology that an institution considers should be able to provide delivery confirmations for every message. Essentially, a reliable, pager replacement solution should be equipped with a time-stamped audit trail, allowing healthcare administrators to view when messages were sent, delivered and read by care team professionals.

With such a mechanism in place, there is no way for recipients to evade important, clinical alerts. It enables a facility to boost its care team's accountability, responsibility and workflow operations.

Question Five: Is the Solution Intuitive? Is it Easy for Users to Easily Get Up to Speed and Use the Technology? Is training provided?

While it may seem self-evident, ease of use and implementation should be another key component for administrators to consider when adopting a secure, messaging platform for their healthcare institution. Indeed, the extent to which a person believes that using a new technology will be free of effort greatly impacts adoption[xi]. Considering how many users will need to adopt the technology, it is important that a pager replacement solution require only a short and simple learning curve.

Equally as important, change agents need to ensure that the technology provides (1) intuitive controls and interface, (2) easy

usability without excessive click-throughs and (3) a strong sense of what its functionality should accomplish.

Further, the technology should be complemented by 24-hour support from the vendor, ensuring that a healthcare administrator's concerns or questions are resolved. Additionally, organizations need to recognize whether or not a considered, technology provider offers comprehensive training. Administrators need to make sure this level of care is provided, allowing healthcare practitioners to receive a comprehensive walk-through of the technology, which in turn, equates to a desired plug and play process.

Question Six: Is There Administrative Control? Can an Administrator Easily Provision the Addition and Deletion of New Users?

It is important for administrators to understand how much control they will have over a newly adopted pager solution. With enhanced technology supervision, administrators can ensure that only authorized users are receiving and delivering messages.

The fact is that 68 percent of healthcare security breaches are attributed to the loss or theft of mobile devices and files[xii]. As such, administrators need to be equipped with technology that provides (1) remote-wipe capabilities and (2) the ability to grant clinical communication access to intended users. As a result, administrators can avert hefty fines placed by HIPAA.

Question Seven: Does the Solution Improve Workflow?

Inefficient workflows caused by the use of pagers have a significant impact on patient care as well as on healthcare cost. According to the Ponemon Institute, time is wasted during each workflow where pagers are used. Use of legacy pager technologies have an estimated annual, economic impact on U.S. hospitals of $8.3 billion annually[xiii].

One of the key attributes of a strong, secure messaging technology is that it improves workflow and decreases length of hospital stay for patients.

As a study noted, patients whose care providers were offered mobile, secure text messaging experienced a decrease in length

of stay[xiv]. The reason for this is that pager replacement solutions offer "communication that allows providers to close the loop quickly and hold group chats that involve the entire care team[xv]."

It is important that administrators adopt and implement a technology that allows for contextual attachments (e.g., voice memos and images). This enables care team members to receive timely, comprehensive information before providing treatment to a patient. Accordingly, healthcare practitioners can execute faster treatment, which decreases a patient's length of stay.

Question Eight: Do You Have Smart Scheduling Capabilities Built into the Technology?

Many traditional hospitals use analog schedules written on a whiteboard in close proximity to the reception room. There are several issues with this legacy workflow, such as (1) delaying contact with doctors or nurses and (2) making it easy to generate unnecessary errors due to faulty manual transcription of contact information.

As a solution, administrators should adopt a clinical communications solution that is equipped with built-in scheduling capabilities. Administrators can upload desired schedules through a solution's web-based console. All scheduling changes or alterations can be completed through a simple-to-use and share electronic scheduler, ensuring that the right on-call care team member receives a critical alert at the right time.

Question Nine: Does the Technology Have a Strong Track Record? How Many Hospitals Have Successfully Used the Technology?

Investing in an effective, reliable and sound technology is not an easy task for healthcare institutions. That is why organizations need to consider and select a clinical communications platform with a proven track record of improving workflow efficiency, HIPAA compliance and collaboration.

During this process, healthcare administrators should also determine whether or not:

- The considered technology has been used in many different types of healthcare institutions
- The considered technology has been effective both in small clinics as well as large hospitals
- The considered technology has been effective for different types of specialties

If the considered technology can answer "yes" to these checklist items, then it can adapt to the many uses of a large hospital or the different needs of doctors at a small, local clinic.

Healthcare administrators need to adopt a clinical communications platform that does not disrupt care team operations. By communicating with vendors and asking for references, healthcare institutions can ensure that they select the right technology for their organizational needs.

Conclusion

Secure messaging solutions are one of the most sought-after-applications in healthcare. However, not all solutions are created equal. The right secure messaging solution will provide more than just a pager alternative and HIPAA compliance. It will also improve workflow, ensure physicians never miss critical alerts and enhance administrative control over messaging.

Do not let secure messaging remain an enigma. Make sure that you ask the questions above when your healthcare institution searches for the right secure messaging and critical alerting solution.

About OnPage

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 notifications needs.

For more information:
Visit www.onpage.com
Contact marketing@onpagecorp.com
Call (781) 916-0040.

SCHEDULE A DEMO!

End Notes

[i] https://www.hcinnovationgroup.com/clinical-it/news/13028930/almost-80-percent-of-clinicians-still-use-hospitalissued-pagers

[ii] https://www.metrotel.com/motorola-advisor-elite-alpha-numeric-pager-free-w-annual-service-order-on-line-or-call-888-441-2616/

[iii] See ii

[iv] https://netdiligence.com/portfolio/cyber-claims-study/

[v] https://www.onpage.com/bullet-proof-scheduling/

[vi] https://www.beckershospitalreview.com/patient-flow/how-to-use-technology-to-align-incentives-and-improve-patient-flow.html

[vii] https://www.onpage.com/healthcare-resource-library/whitepaper-why-pagers-suck/

[viii] http://it.emory.edu/mobileconnect/RisksofPagingandSMS/index.html

[x] https://www.beckershospitalreview.com/hospital-management-administration/thoughts-on-big-threats-for-hospitals-today.html

[xi] https://www.cluteinstitute.com/ojs/index.php/IJMIS/article/download/9086/9091

[xii] https://www.accellion.com/blog/lost-stolen-mobile-devices-leading-cause-of-healthcare-data-breaches/

[xiii] https://www.hcinnovationgroup.com/clinical-it/clinical-documentation/news/13021199/study-pagers-outdated-communication-tech-costing-hospitals

[xiv] https://www.ncbi.nlm.nih.gov/pubmed/27016064

[xv] https://mhealthintelligence.com/news/text-messaging-study-shows-clinical-benefits