# REPLACING PAGERS TO IMPROVE PHYSICIAN ACCOUNTABILITY

# REPLACING PAGERS TO IMPROVE PHYSICIAN ACCOUNTABILITY

In a recent article written by Providence Community Health Center's CMO, Dr. Andrew Saal wrote that one of the major issues his hospital faced when physicians were using pagers was a lack of personal accountability. According to Dr. Saal,

*There w[ere] issues with professional accountability (when physicians used pagers). One would often hear:* "I had the pager turned on, but it never went off. It must be the fault of the aging network… or maybe the answering service"

What this incident highlights is that by using pagers, physicians had and continue to have a readily available crutch - a crutch they could use to explain why they did not respond to patient requests or to explain why they did not *respond* to colleagues requests. And while there was no way to verify if these statements were excuses or valid explanations, the result was the same. In the moment of need, the on-call physician could not or did not respond.

What also comes to light in this instance is that if a hospital is to run efficiently, **on-call must be accountable**. Otherwise, too many important calls can fall through the cracks. Additionally, physicians need to be accountable when they are on-call and when their patients need them.

The goal of this whitepaper is to highlight how secure physician messaging improves accountability and overall patient outcomes. To that end, this whitepaper will examine:

- What secure physician messaging is
- How secure physician messaging is better than pagers
- How secure physician messaging **improves accountability**

## SECURE PHYSICIAN MESSAGING

Secure physician messaging refers to messaging that ensures the secure exchange of patient information – often referred to as protected health information (PHI) – between physicians. By using secure physician messaging, practitioners ensure that information is exchanged via a secure and encrypted platform which adheres to the mandates of Health Insurance Portability and Accountability Act (HIPAA) regulations.

Failure by practitioners to use a HIPAA secure messaging application when exchanging messages with colleagues that contain PHI can constitute a HIPAA fine. Indeed, HIPAA officials have cited health facilities for exchanging PHI that was neither encrypted nor password protected. If and when a HIPAA fine is instituted, the fine can reach several million dollars.

Due to the risk of rebuke and the potential fine that can ensue from exchanging unsecured patient information, many hospitals – including Dr. Saal's Providence Community Health Center - and clinics have chosen to adopt HIPAA compliant messaging applications. These hospitals and clinics have realized the limitations they face and risks they bring on by using traditional pagers. These groups have also understood the benefits that HIPAA secure messaging can bring in terms of expediting patient care, improving patient outcomes and reducing healthcare costs.

## BETTER THAN PAGERS

Pagers have many faults, not least is their inefficiency which costs the average hospitals $1.75 M per year in inefficient communications and can impede critical clinical workflows.  Pagers lack critical functionality specifically focused on the following seven points:

- *Pagers are not encrypted*: Pagers do not provide encrypted communications. Without encrypted communications, HIPAA compliant messaging is extremely difficult in a healthcare setting. Communications on pagers must be extremely limited and non-descriptive if doctors are to use them and not violate HIPAA regulations.

- *Pagers can be hacked*: According to a recent case study, a U.S. based hospital had their pager communications hacked and red by outside parties that forced the hospital to register the violation with the Department of Health and Human Services

- *Pagers only have high priority pages*: Pagers typically don't have low versus high priority messaging. In a world where all you have is a hammer, every page looks like a nail.

- *Pagers have a limited range*: This limitation goes to the heart of physician accountability as outside of the few square blocks neighboring a hospital, a physician often won't receive their intended page.

- *Pagers don't enable two-way communication*: Pagers can often only receive pages but not initiate or further communication. This flaw further highlights the lack of accountability perpetuated by pagers. If physicians cannot delve into a request, they often are left with partial and incomplete information.

- *Pagers cannot escalate alerts*: For pages that are critical, there is frequently the need to bring in expertise or assistance of other professionals. Traditional pagers don't permit this level of communication to occur.

- *Pagers don't allow attachments*: Successful healthcare diagnoses and effective treatments typically require test results and imaging. However, traditional pagers are incapable of facilitating this necessary level of communication.

Secure physician communications like that provided by OnPage's platform do permit physicians to exchange encrypted attachments and messages. Additionally, physicians are able to escalate alerts and communicate in a robust manner – all capabilities which run opposite to the limited functionality of pagers.

## SECURE PHYSICIAN COMMUNICATIONS IMPROVE ACCOUNTABILITY

1. **Audit trail**: As noted in the previous section, physicians are often not accountable because their pagers are unable to receive messages in many parts of the hospital as well as beyond the few blocks surrounding the hospital. Consequently, if the answering service or a colleague tries to page a physician, the physician can easily not hear the page or easily ignore it. With secure messaging platforms like OnPage however, answering services and colleagues can actually see if the physician who is being sent the message has received the alert. This assurance enables senders to know that their message has been received and if it has been read.
2. **Presence information**: Clinicians are at times known to be "digitally missing in action". That is, the clinician who is supposed to be on-call does not have their device operational or logged on so they cannot be reached. Secure messaging platforms however allow the sender (either the on-call service or a colleague) to see if the practitioner to whom they are sending the message is actually logged in. This characteristic of secure

messaging platforms improves accountability since if the physician is not logged onto the application he or she can easily be called and told that they need to log in.

3. **Accountability is increased with alerting. Higher possibility of reaching colleagues:** It sometimes occurs that when a physician is paged they are either unable to respond to the alert or do not hear the alert. Unfortunately, this inability of pagers to provide persistent alerts makes it easy for alerts to be forgotten or missed entirely. Secure messaging platforms however provide persistent alerting that continues for several hours if the practitioner does not immediately respond to the alert. With this persistent alerting component, physicians are inevitably more accountable to colleagues because they can neither forget nor avoid their colleague's need for help.
4. **Personal information remains encrypted. No violation of trust:** Part of physician accountability is maintaining the confidentiality of patients. If a physician is using a pager however, he or she can easily exchange privileged and sensitive patient information that has no encryption to secure it. As a result, if the pager is picked up by another patient or anyone who is not authorized to see the content, the patient's confidentiality has been violated. Secure messaging platforms however enable physicians to maintain this level of confidentiality by putting several layers of encryption over the information.
5. **Improves relay of messages**: As secure physician communication platforms expedite messages and attachments there is inevitably less delay in the exchange of important patient information. As a result, physician are more accountable to their patients because they have access to updated information that has relevant attachments and clarifications to enable the best patient treatment possible.
6. **HIPAA compliance:** An extremely important aspect of secure physician communications is maintenance of HIPAA compliance. By not heeding the mandates of HIPAA compliant communications, hospitals can experience significant fines. For example, in 20016 Catholic Health Care Services was fined $650K for failing to have patient information encrypted and password-protected. Transmitting patient information over an unsecured network is inviting a HIPAA disciplinary action or fine. It is incumbent upon all physicians to comply with HIPAA and be accountable to the demands of HIPAA. This level of accountability is ensured with secure physician communications.

## CONCLUSION

Eliminating the use of pagers in healthcare will significantly improve physician accountability.  As noted throughout this whitepaper, pagers enable physicians to miss critical messages and potentially violate HIPAA statutes. It is incumbent upon healthcare facilities to make physician accountable to their colleagues and their patients. In order to achieve these ends, physicians and hospitals must end their relationship with pagers.

## ONPAGE CAN HELP

The causes of alert fatigue have been well documented in this report. Alert fatigue is due to the excessive number of alarms, alerts and resulting cognitive overload put on hospital staff. As noted, the inability to correctly bring the important alerts to the top impacts the quality of care which patients receive and could even result in dire consequences.

However, when practitioners have access to tiered alerting and communications methods such as the powerful and robust clinical communications platform provided by OnPage, they can minimize the number of inactionable and inconsequential alerts. Additionally, they can minimize the chance for errors.

OnPage's **HIPAA complaint** critical messaging service enables healthcare providers to receive alerts via encrypted and secure text communication methods. OnPage messages are **SSL encrypted** and can only be viewed by message participants. Furthermore, OnPage has **remote wipe** capabilities to further ensure HIPAA compliance.

By decreasing the number of false alerts that physicians and nurses receive, OnPage can significantly decrease the level of practitioners' alert fatigue and improve overall patient care.

Contact OnPage to learn more about how we can help you with your IT needs.

TO LEARN MORE, VISIT OUR WEBSITE OR CALL: ONPAGE.COM

CONTACT- US 781-916-0040 OR DOWNLOAD THE APP

Available on the App Store

Get it on Google play