The Perils of Pagers in Clinical Settings

$30 Antenna Picks up Private Patient Info

In June of this year a Missouri man, using an antenna to pick up TV channels on his laptop, was surprised to see unencrypted patient information from both local and distant hospitals.

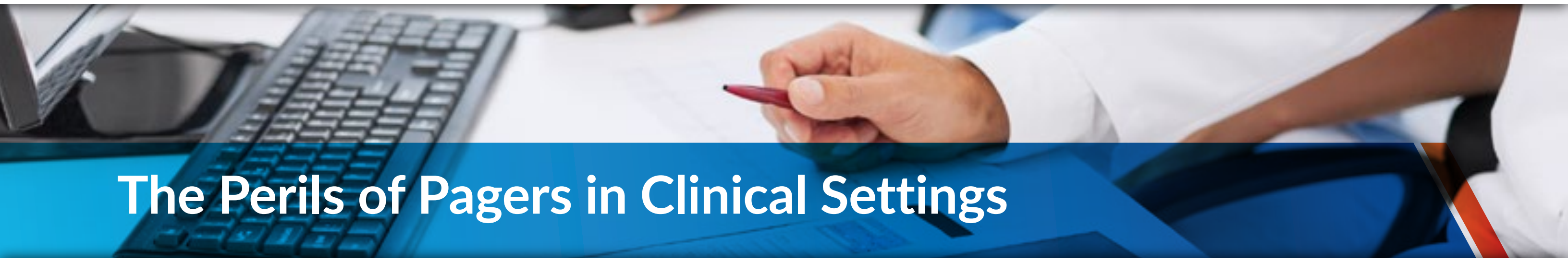
Reported by **The Kansas City Star**, the man, using free software and a $30 antenna, began seeing private clinical information including:

RQSTD RTM: (patient's name) 19 M Origin Unit: EDOF Admitting: (doctor's name) Level of Care: 1st Avail Medical Diagnosis: TONSILAR BLEED, ANEMIA, THROMBOCYTOPENIA

What happened?

It turns out that a $30 antenna can pick up radio signals that are digitized, such as signals sent to pagers. The big news in this story is that the man picked up Protected Health Information (PHI) from multiple hospitals, both near and far, at the same time. They were unknowingly broadcasting patient information in a way that virtually anyone could pick up.

This recent example is, unfortunately, all too familiar in hospitals. In a day and age when digital privacy technology is both widespread and affordable, hospitals are still using pagers and unsecured texting to relay sensitive patient information.



Black Market for EHRs

On the black market, a patient's EHR can be worth hundreds, even thousands, of dollars. A typical EHR often contains the most comprehensive private data ever compiled about an individual. A patient's name, address, work history, names and addresses of relatives, financial information including credit card and bank numbers, are all contained in EHRs.

Medical data thieves often have a larger motive than re-selling a patient's private information: blackmail. If a patient's records contain sensitive information such as cancer diagnosis, sexually transmitted disease or mental health issues, a clever blackmailer can extract payments from an individual for a long time.

According to **Forbes**, in 2016 there were 450 EHR breaches, affecting 27 million patient records. Of these, more than 25% originated with outside hackers.

More Downside

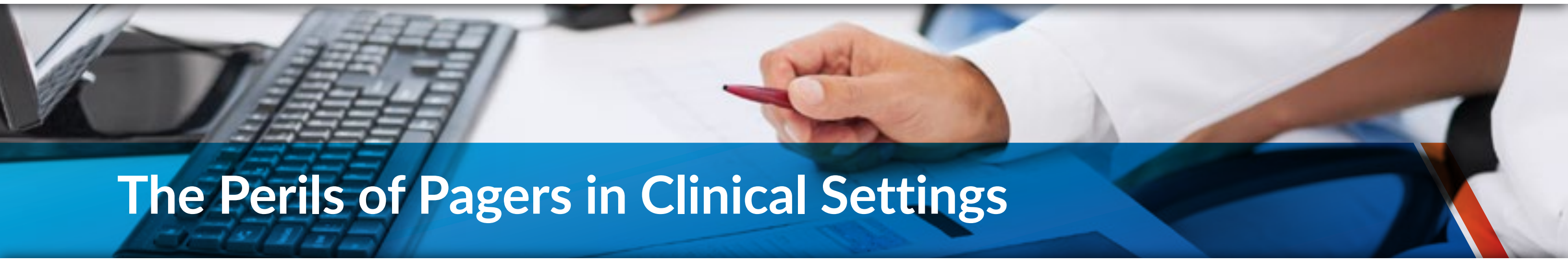
Aside from cybersecurity issues and related HIPAA violation penalties, there's even more downside to using outdated communications devices in clinical settings.

Efficiency - Send a page, call someone back, leave a message, play phone tag. The average provider or nurse wastes 45 minutes per day answering pages. Multiply this by the number of nurses and other clinicians using pagers and you begin to get a feel for the time wasted trying to communicate this way.

Patient Safety - You may be familiar with the phrase "page and pray" that was coined based on legitimate problems closing the loop in a paging system. Statistics show that 1 in 7 pages are sent to the wrong person and that 30% of pages go unanswered within the first 15 minutes.

Accountability - Do you know if or when a page was sent, or whether it was ever successfully delivered or viewed? The Joint Commission found that two out of three medical errors are caused by a breakdown in communications. In a paging system there is no transparency and no visibility into the communication data of your organization, which means there's no basis for accountability or ability to address breakdowns in communication.

Compliance - Texting is a nearly ubiquitous form of communication and that trend is not going away. However, organizations without a secure communication tool in place will likely find that their users are texting via non-secure means. Data shows that 75% of providers are texting via unsecure means and 53% of breaches are from mobile devices.



The Perils of Pagers in Clinical Settings

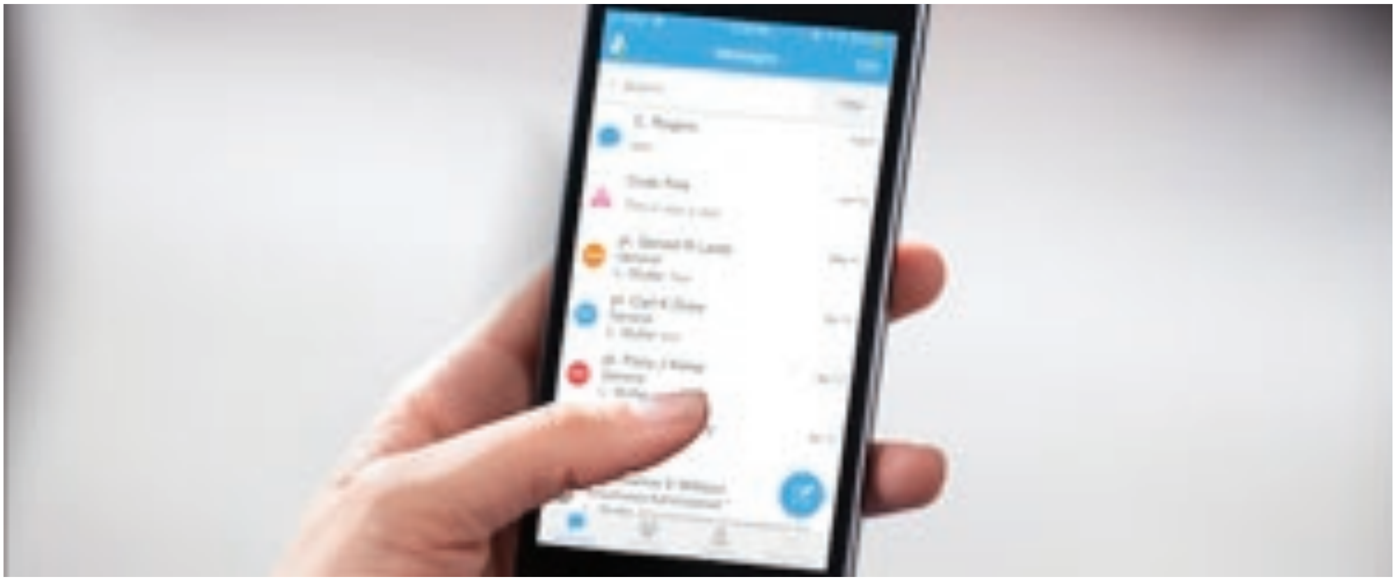
Secure Communications Platforms in Healthcare

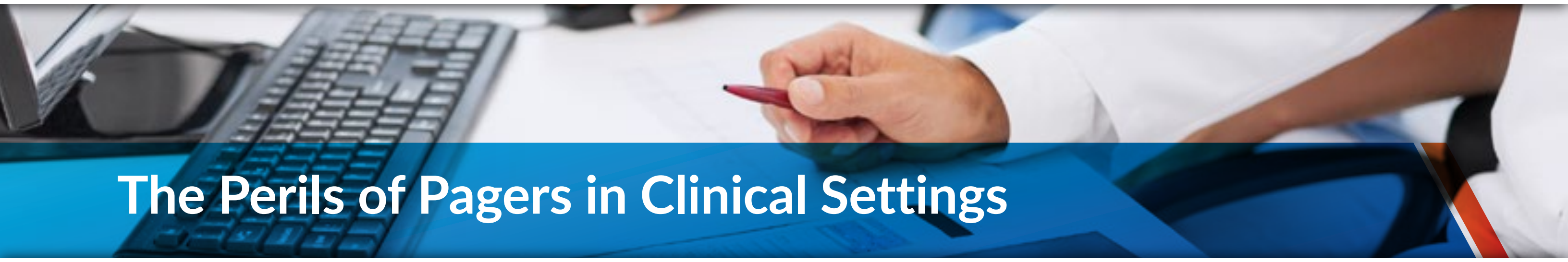
While it's true that many healthcare providers have switched to texting, industry estimates indicate that 70 percent of them are currently texting unsecurely.

Most hospitals today are looking to replace a tangled web of landline phones, mobile phones, pagers, handheld radios and overhead paging with a platform that meets or exceeds today's cybersecurity standards. If your team is looking for a new solution, the following information will be useful.

A secure healthcare communications platform should contain these security features:

- **Stream data on the fly with no PHI persisting on the end user devices**
- **All intra and inter-system transmissions are encrypted via 256-bit Advanced Encryption Standard to protect data in transit**
- **Extensive role-based permissions and administrative controls to provide application access as needed**
- **Leverages event sourcing to provide a tamper resistant database**





What to Do Next

The best place to start is within your own department. Take an informal survey of the types and quantities of older devices in use. Pick 10 people in your department that send or receive PHI on mobile devices, and ask them:

1. What are the makes and models of devices you currently use on a daily or weekly basis?

2. Do you know whether PHI is encrypted, and how so?

Next, **review some of the offered solutions** to see which one(s) could help with your cybersecurity needs. Once you've narrowed down the list of vendors, engage your IT and finance teams to help determine next steps, including system compatibility and required ROI.

The next step is to **engage the vendors**, sharing what you believe to be your organization's clinical communication priorities and purchase criteria.

Setting and maintaining appropriate levels of secure communication protocols in clinical settings is not just the IT department's responsibility.

It's yours too.

About the Author

James F. Baxter is CEO of Nashville-based MEDarchon, a leader in healthcare communications systems. His career includes a long tenure in healthcare technology management and consulting, CRO and clinical lab work with ClinTrials Research, Inc. and SmithKline Beechman Clinical Laboratories and managed care experience at American Medical Plan. Baxter is a graduate of Vanderbilt’s Owen Graduate School of Management.