Don't Let Pagers Blindside your Privacy and Security Program

By Julie Roth, JD, MHSA, RHIA

Imagine the following scenario. Jane has served as the HIPAA security officer for a 200-bed community hospital for five years. Fortunately, the hospital's governing board understands the importance of HIPAA compliance and provides the health information management (HIM) and information technology departments with the resources necessary for a comprehensive HIPAA privacy and security program.

Written policies and procedures are in place and staff receive HIPAA training at the time of hire, followed by periodic HIPAA updates. Processes are in place to audit workforce members' access to protected health information (PHI) and the hospital has deployed encryption, firewalls, and other technical safeguards to ensure that electronic PHI (ePHI) is not compromised. While occasional incidents may occur, Jane considers the hospital's privacy and security program to be one of the most robust in the area.

Then, it happens. Jane receives a telephone call from a reporter for the local newspaper who explains that he is in possession of copies of patient information that was communicated via pager messaging between hospital employees. A concerned citizen who had intercepted the pager messages provided the reporter with the copies, which include details such as patient name, age, diagnosis, and location within the hospital. As the reporter asks for Jane's comment, she realizes that he has already contacted some of the patients involved and that the story will soon be front page news.

Several questions rush to Jane's mind. Pagers are used to convey detailed PHI? How were the pager communications intercepted and who is in possession of the information? What will the regulatory consequences be? And, most importantly, how can vulnerability presented by pagers be stopped?

This scenario was recently the alarming reality for several Midwest hospitals, and highlights the significant security risks and potential fallout presented by an often-overlooked communication technology still utilized in many healthcare facilities: the pager.[1]

Pagers Still Used to Communicate PHI

While many people may believe that "old school" radio wave pagers died out with the introduction of smartphones, they are actually still used with surprising frequency in healthcare. Because pagers transmit data via radio waves, they are not dependent on a cellular signal or wireless network connection to work. Furthermore, pagers can instantaneously display words and sentences, as opposed to a mere call-back telephone number. Thus, pagers can serve as an important means of communication for providers in areas of hospitals where a wireless or cellular signal is weak, slow, or potentially disruptive to medical equipment.

Security Risks Presented by Pagers

Although pagers can be an important means of communication, the unfortunate reality is that many pager messages are easily intercepted and retained by anyone with a computer, inexpensive hardware, and software-defined radio. Intercepted messages have not only been posted on the internet, they have been the subject of research studies,[2] curious "hobbyists,"[3] and even art installations.[4] These instances demonstrate that pager messages may include details such as a patient's name, age, location, treating physician, and diagnosis.

The interception of pager messages containing PHI not only triggers a hospital's duty to determine if a breach notification is necessary, but it may expose the hospital to civil penalties imposed by the Office for Civil Rights (OCR) for the failure to

properly secure PHI. Moreover, such an incident can be damaging to a hospital's reputation by eroding the public's trust that the hospital will protect patient information from unauthorized access.

Addressing the Risk

The HIPAA Security Rule requires covered entities to implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. Penalties for violating the HIPAA Security Rule can range from $114 to $57,051 or more per violation.

ePHI includes PHI that is maintained or transmitted by electronic media. OCR defines "electronic media" to include "transmission media used to exchange information already in electronic storage media." According to OCR, "transmission media include, for example, the internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media *if the information being exchanged did not exist in electronic form immediately before the transmission."*

Because most pagers transmit information that exists in electronic form immediately before the transmission, the transmitted information constitutes ePHI and is subject to the HIPAA Privacy and Security Rule standards.

Under the HIPAA Security Rule, a hospital or other covered entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI. Given how readily pager communications can be intercepted, any risk assessment should consider whether ePHI is communicated using pagers. A covered entity must also address any security measures that are necessary to ensure that ePHI is not improperly modified without detection during transmission.

Again, this standard includes transmission of ePHI via pager. Additionally, covered entities should address a mechanism to encrypt ePHI whenever deemed appropriate, and again include pager messaging in this assessment, according to HIPAA.

The bottom line is that hospitals and other healthcare providers who use pagers should either refrain from transmitting PHI via pager or acquire a secure pager or other messaging system that is capable of encrypting PHI during transmissions.

Notes

1. Marso, Andy and Kelsey Ryan. "Does your hospital still use pagers? Your personal information may be at risk." *The Kansas City Star*. June 22, 2018. www.kansascity.com/news/business/health-care/article213414334.html.
2. Trend Micro. "Leaking Beeps: Unencrypted Pager Messages in the Healthcare Industry." 2016. www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-leaking-beeps-healthcare.pdf.
3. Marso, Andy and Kelsey Ryan. "Does your hospital still use pagers? Your personal information may be at risk."
4. DaCosta, Marc. "How to Explore the Hidden World of Radio Waves All Around You." December 18, 2017. Motherboard. https://motherboard.vice.com/en_us/article/59wpmn/how-to-explore-the-hidden-world-of-radio-waves-all-around-you.

Julie Roth (jroth@spencerfane.com) is a partner at Spencer Fane LLP in the firm's Overland Park, KS office. She helps healthcare providers through a variety of transactional and regulatory matters and represents large health systems, hospitals, and physician practices, and counsels clients on regulatory compliance matters.

Legal eSpeaking Blog Examines Legal Impacts on Health Information Management

http://journal.ahima.org/category/blogs/legal-e-speaking

The *Journal of AHIMA*'s Legal eSpeaking blog highlights judicial decisions and regulatory initiatives, among other legal-related topics, that may impact AHIMA and its members. From the continuing scourge of data breaches to emerging sources of electronic health information, 2019 promises many further developments in this arena.

Data breaches, enough of a headache on their own, may translate into a costly liability for healthcare providers. More judicial responses to data breaches can be expected in the coming year, underscoring the need for data security. And as health information technologies continue to proliferate, such as apps that record and transmit vital signs and other health information, it's important to consider relevant questions in this evolving field, such as: Will the developers or marketers of the apps be subject to HIPAA? How will healthcare providers integrate information from such sources into existing information governance structures?

Legal eSpeaking will focus on these and other developments in 2019 and introduce readers to how the law may respond to and impact new challenges and technologies for health information management.

Article citation:
Roth, Julie. "Don't Let Pagers Blindside Your Privacy and Security Program." *Journal of AHIMA* 90, no. 2 (February 2019): 34-35.