Health Information Compliance Alert

Compliance: GI Firm Exposes Patient Data Due to Device Incompatibility

Tip: Ensure your systems and devices match up.

The more technologically advanced medical practices become, the more training, resources and equipment are required. But when that IT breaks down, we often have to find a workaround - and although that can be a boon for interoperability, it can create privacy issues.

That's the lesson that gastroenterology staff members at a **Veterans Affairs** hospital in California recently learned, according to a July 31, 2019 report by the VA's **Office of Inspector General** (OIG).

Incompatible Systems Drove the Issues

The problems that the OIG found stemmed from the fact that the facility's high-resolution esophageal manometry (HRM) device was unable to interface with the VA's EHR system starting in 2013.

"The gastroenterology (GI) provider stated that, along with the facility Biomed and IT, a decision was made to continue to use the facility's HRM without the ability to interface with the patients' EHR," said **John D. Daigh, Jr., MD**, **VA-OIG** assistant inspector general for healthcare inspections, in his report. "Based on this decision, the GI provider developed and implemented two workarounds that were not in accordance with VA security and privacy policies concerning sensitive personal information. These workarounds included the use of the GI provider's personal computer and emails, a non-VA (unencrypted) flash drive, and the Cloud."

The way the GI staffers transferred information between the two systems led to a breach of patients' private information. In fact, 99 percent of the emails that the gastroenterologist sent from his personal email account contained patients' sensitive personal information, as did 91.7 percent of texts between the GI provider and staff members.

Outcome: In total, the OIG pinpointed 133 patients whose sensitive personal information was cited in emails and text messages from the GI provider to staff members. The OIG determined that the situation did not meet the criteria for a formal breach notification, but the facility was at risk of disclosing their personal information.

"A complete/full risk assessment would have shown a possibility of disclosure based on the ease to obtain the information and the length of time the unencrypted information remained on an unprotected site," the report noted.

Here's How to Avoid A Similar Fate

If your practice is considering using personal text, email or other accounts in the office, make sure you stay within the regulations with a few quick tips.

Educate staff: The first step your practice should take involves devising a comprehensive plan that includes realistic procedures to combat the accidental and intentional loss of electronic protected health information (ePHI).

Educating administrative and clinical staff on the rules related to HIPAA-compliant communication via text, interoffice messaging, and email is essential to keep your practice safe and secure. That includes integrating user-friendly software and applications across the different mobile products your group utilizes to ensure the success of your overall plan.

Apps: It's important that the applications you use for texting and to message patients as well as your associates meet healthcare industry standards for security and privacy during the communication of ePHI. Additionally, with text messaging, and due to the features included in secure messaging solutions, it ensures that system administrators can audit access to encrypted ePHI and any transmission of confidential data in compliance with HIPAA regulations.

Pocket these seven tips for managing mobile devices in your practice:

- Eliminate the threat of sensitive data being compromised if a mobile device is stolen or lost with message recall, message lifespan, and remote wipe.
- Segregate healthcare texting from personal texting through a HIPAA-compliant, secure application.
- Encrypt message data in-network and in-transit on the device and the server.
- Look for a lockout feature that erases data remotely if devices are stolen.
- Require multifactor authentication (MFA) for all application users.
- Include configurable time-out periods.
- Block users after a number of unsuccessful authentication attempts.

Bottom line: SMS texting is not encrypted or secure, yet providers unwittingly engage in the practice of texting often, leaving their patients and themselves vulnerable to cyberattacks and the loss of ePHI. Due to the confusing nature of the policies, it is wise to seek the advice and assistance of healthcare IT experts schooled in the complexities of the HIPAA Security Rule and its regulations.

Resource: To read more about the case, visit www.va.gov/oig/pubs/VAOIG-17-03557-177.pdf.