

## Health Information Compliance Alert

### Reader Questions: Keep Patients Aware of Medical Device Cyber Risks

**Question:** With the uptick of cyberattacks during the COVID-19 public health emergency (PHE), should we be concerned about our patients' medical devices being hacked?

Georgia Subscriber

**Answer:** Yes, medical device safety has become a major concern with so many providers tracking patients' progress through applications and devices during the pandemic; the risks have increased exponentially. In fact, the U.S. Food and Drug Administration (FDA) issued a new brief, "Best Practices for Communicating Cybersecurity Vulnerabilities to Patients," in October that focuses on relaying information about a device's vulnerability to patients and how to communicate these issues in case of a cybersecurity breach.



**Reminder:** The Internet of Things (IoT) has been a great boon to the healthcare industry, allowing the connection of devices, systems, and objects to the Internet to differentiate and enhance patient care and provider coordination. This bridge between devices, practitioners, and patients supports the idea that connecting everything in your office - and life - will make practicing medicine more efficient, effective, and easier; but, that's not always the case. With each new hook up, the opportunity for the loss of electronic protected health information (ePHI) increases.

If you are implementing a cybersecurity plan for your medical devices, consider these FDA tips on communicating vulnerabilities to patients:

- Utilize simple terminology to explain why a medical device might be ripe for a cyberattacks and how to identify a security issue.
- Use text messaging, email, EHR, and social media to let patients know if there's an outage or data risk on certain devices.
- Issue alerts in diverse languages to make your communication more inclusive.
- Explain the benefits of medical device security to better allow patients to determine when they should alert providers about a cyber issue.
- Ensure medical device functionality, name, manufacturer, and FDA updates are readily available to your patients in case vulnerabilities are identified.

**Resource:** Review the FDA guidance at [www.fda.gov/media/152608/download](http://www.fda.gov/media/152608/download).