# Health Information Compliance Alert

## Cybersecurity: FDA Offers New Incident Response Ideas for Medical Devices

**Tip: Keep medical devices off the network if possible.**

Recent studies point to the importance of incident response plans to combat data breaches in healthcare. Strong mobile device management has been shown to not only protect patients, but also save practices money when a breach occurs.

Now, the U.S. Food and Drug Administration (FDA) wants to get involved in the cybersecurity game with a new program to address medical device security after an attack.

**History:** In May of 2017, the United States suffered from the fallout of a large-scale ransomware infiltration that fanned out across the globe. As the situation escalated, clinicians and hospitals had to turn away patients because they couldn't access medical records. The "WannaCry” cyber attack allowed hackers a doorway into systems worldwide then demanded payment in bitcoin to decrypt the data.

**Nuts and bolts:** During and after the WannaCry shutdown, the FDA discovered from stakeholder feedback that healthcare and public health (HPH) infrastructures and healthcare delivery organizations (HDO) were concerned about the security of their medical devices, suggests FDA guidance. In an effort to address these worries, the FDA enlisted the MITRE Corporation to put together a regionally-based resource for clinicians faced with securing their medical devices, which are essential for clinical work and vulnerable when systems are under attack.

Last week, MITRE and the FDA released Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook "to understand the gaps, challenges, and resources for HDOs participating in medical device cybersecurity preparedness and response activities,” notes the report's introduction.

### Even Smaller Providers Must Protect Their Medical Equipment

One of the primary focuses of the Playbook targets "user awareness training.” All staff "from clinicians to IT helpdesk staff and HTM professionals, should be aware of potential device cybersecurity incidents, their impacts, and appropriate responses,” the FDA/MITRE report advises. The agency guidance points out that many cyber attacks are actually discovered by device users.

"Cybersecurity issues often initially manifest as unusual device behavior,” which is why "regular training for device users will help to ensure that cybersecurity is considered as a potential cause for any device peculiarity,” according to the Playbook.

### Put Together an Incident Response Plan for Your Practice Medical Devices

Large-scale attacks like WannaCry and Petya that take down entire hospital systems are rare, but that doesn't mean you shouldn't prepare for the worst, especially when it comes to securing devices used to monitor and care for patients. Putting measures into place now that protect your patients later will not only save you money, but it may save lives, too.

Here is a list of the top ten things that **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC** in Charlotte, Vermont, advises clinicians to consider when planning their medical device management and incident response plans:

> **1.** Inventory all the medical devices thoroughly, including vendor contact information and the ability to patch or update the device's security.

**2.** Point out which devices are able to be updated for security and plan for regular checking and application of updates.

**3.** Determine whether or not the data on the devices needs to be backed up, or needs to be cleared if the device is returned to the vendor, and plan for these as necessary.

**4.** Lock down all access to medical devices to the extent practicable and turn off all default passwords.

**5.** Do not connect devices to networks unless it is necessary for their operation or maintenance, and disconnect them from networks when not in use.

**6.** Provide a separate logical subnet for medical devices as practicable, to separate the devices from other systems and networks.

**7.** Stock spare backup units for critical functions, using units of a different maker or type, to be able to maintain services if some units are compromised.

**8.** Develop mutual-aid plans for borrowing equipment as needed during incidents from nearby entities, including setting up separate secure networks on an emergency basis.

**9.** Review and update your incident response and contingency planning policies and procedures to ensure the consideration of medical devices and the Internet of Things.

**10.** Ensure medical devices and the Internet of Things are included in risk analyses and management planning.

**Resource:** Read the FDA's Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook at www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf.