Medical Device Cybersecurity
HELPING TO KEEP PATIENTS AND MEDICAL DEVICES SAFE

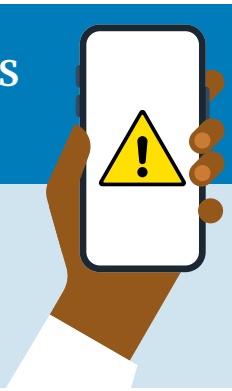
Medical device cybersecurity is patient safety. Cybersecurity incidents can affect patients by impacting medical device availability and functionality. Managing cybersecurity risks is critical to ensuring safe and effective medical devices for everyone.

One way the U.S. Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH) supports this key focus area is through its medical device cybersecurity team. This team helps keep patients safe through a variety of ways, such as making sure that medical devices meet cybersecurity requirements.

To mark the team's 10-year anniversary, here is a look at some of the ways they have contributed to patient safety over the past decade:

17 SAFETY ALERTS ISSUED

CDRH issued alerts about significant cybersecurity concerns to help minimize impacts to patient care.



479 VULNERABILITIES IDENTIFIED

Public and private partners, including CDRH, identified, responded to, and acted to mitigate vulnerabilities to proactively protect patients.

13 CYBERSECURITY INCIDENTS MANAGED

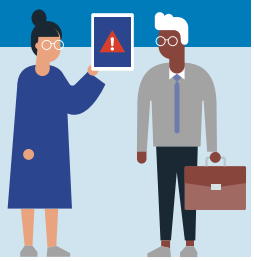
CDRH responded quickly to address medical device cybersecurity incidents.

31 CYBERSECURITY RESOURCES PRODUCED

CDRH, in collaboration with partners in this sector, developed publications and best practice documents for health-related stakeholders, including patients.

68 CYBERSECURITY-RELATED RECALLS ISSUED

CDRH analyzed cybersecurity concerns and worked with industry partners to address recalls to ensure medical device safety and reliability.



6 CYBERSECURITY TEAM MEMBERS ADDED

CDRH grew its cybersecurity team to respond to a growing number of potential threats, collaborate with stakeholders, and support medical device safety.

For more information on how to keep medical devices safe, visit www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.