Testing medical connectable devices to cybersecurity standards

The pervasive use of digital technology brings many benefits, but it can also be problematic. “Digital technologies increasingly touch the most sensitive aspects of our lives, providing convenience but also creating new, often unforeseen risks,” notes the United States’ National Cybersecurity Strategy, published in March 2023.

This risk is especially prevalent in the field of medical information, as the healthcare industry is a significant target for hackers and cybercriminals. These bad actors could compromise private and confidential healthcare data and endanger the safety and health of patients.

Any risks associated with the operation of medical devices must be acceptable to enable a high level of protection of health and safety, according to Annex I, Section 1 of the Medical Devices Regulations. This can only be achieved through the establishment of an adequate balance between benefit and risk during all possible operation modes of a medical device. To this end, there is a need to consider the relationship between safety and security as they relate to risk.

The UL Cybersecurity Assurance Program (CAP) is designed to help organizations manage their cybersecurity risks, data privacy and interoperability issues — all while confirming their capabilities to the marketplace. Based on the UL 2900 Series of Standards and other industry guidelines, the full suite of UL Solutions’ cybersecurity services supports manufacturers, end users, and system installers and integrators in promoting good cybersecurity hygiene in designing, manufacturing, installing and maintaining medical devices.

Our medical device penetration testing services include vulnerability scanning and binary analysis, protocol and packet analysis of communications, examining security controls and circumventing security features, and working to ward off cryptography attacks.

Other services include:

- Private security workshops to share best practices and learnings unique to your needs
- Gap analysis services to detect non-conformities and errors early in the design phase
- Custom testing and assessment services throughout the development lifecycle
- Complete evaluation and certification services to the U.S. Food and Drug Administration–recognized UL 2900 Series of Standards and other industry-leading standards

The services are highly customizable depending on your specific cybersecurity and organizational needs.

UL Solutions

Principles assessed include

- Development life cycle
- Risk management
- Information security
- Verification
- Validation
- Confidentiality
- Integrity
- Availability

Our testing and certification services apply to, but are not limited to, the following types of connectable devices:

- Medical devices and accessories
- Medical device data systems
- In vitro diagnostic (IVD) medical devices and accessories
- Health IT devices
- Wellness devices
- Software as a Medical Device (SaMD), such as mobile applications, web applications, cloud solutions, etc.

Visit UL.com/Healthcare-Cybersecurity to learn more.

UL Solutions

Safety. Science. Transformation.™

IMS23CS1072117