Healthcare Cybersecurity

Healthcare industry cybersecurity breaches may cost human life

The integration of advanced information technologies in medical devices is transforming the healthcare industry, driving dramatic improvements in the efficiency and effectiveness of healthcare and related services. But this integration has fostered the emergence of a new set of challenges for patients, healthcare providers and device developers and manufacturers. Today, the healthcare industry is a significant target for hackers and cybercriminals, potentially compromising private and confidential healthcare data and placing the safety and health of patients at risk.
Healthcare cybersecurity trends and challenges

Collaborate with UL Solutions
Your cybersecurity journey along the medical device development lifecycle

1. **Advisory**
   - Understanding the healthcare cybersecurity landscape

2. **Training**
   - Understanding regulatory and standard requirements

3. **Gap analysis**
   - Identifying cybersecurity risks and gaps
   - Mitigating risks and gaps by strengthening cybersecurity posture

4. **Certification**
   - Achieving regulatory approval and market access

5. **Lifecycle management**
   - Maintaining secure operations during the entire lifecycle

- **Protect human life**
- **Benchmarking**
- **Brand protection**
- **Risk and cost control**
Healthcare cybersecurity solutions

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

UL Cybersecurity Assurance Program (UL CAP) — A full suite of advisory, testing and certification services is designed to help organizations manage their cybersecurity risks and validate their cybersecurity claims.

Advisory
- Customized program
- Education support
- Cybersecurity best practices and standards
- Assess cybersecurity objectives and processes
- Qualify risk
- Product development

Testing
- Penetration testing
- Structured security assessments
- Exposing software vulnerabilities
- Embedded systems analysis and firmware evaluation

Certification
- Highest recognition of due diligence
- Product or system

UL CAP Cybersecurity Assurance Program
Based on the UL 2900 Series of Standards | UL 2900-2-1

Medical device penetration testing services — Extends from medical device software security testing through authoring the FDA recognized UL 2900 Series of Standards.

Vulnerability scanning and binary analysis
Protocol and packet analysis of communications
Examining security controls and circumventing security features
Cryptography attacks

Medical Device Penetration Testing

Medical device cybersecurity certification — Verify compliance to requirements by validating that product and systems offer a reasonable level of protection against risk.

US FDA
Europe
Medicines Agency
Australia TGA
China NMPA
Fuzz, patch and malware, product testing
Gap assessments
Informative, summative and other testing reports

Medical device cybersecurity certification
Remote support available — sample management, witnessing, video conferencing, virtual engineer, 1:1 document reviews
Why UL Solutions for cybersecurity?

- Independent, trusted third party
- Full life cycle solutions
- Hardware- and software-based security evaluations
- Assessment of security development practices
- Cybersecurity expertise
- Industry knowledge
- Cybersecurity and safety
- Global teams and local support

Cybersecurity foundation

- Expertise in global standards and frameworks
- Extensive knowledge of best practices
- Growing list of Internet of Things (IoT) security solutions

Learn more and speak to one of our experts today at UL.com/healthcare-cybersecurity.