Cyber Security Assurance
Safeguarding Patient Data

The Internet of Things is changing how medical care is being delivered.

The Internet of Things is changing how medical care is being delivered. Remote monitoring by doctors and self-monitoring by patients are becoming common-practice for those that are less mobile or need increased medical supervision. Real-time data on patients is being collected like never before and at the same time, the industry has seen an increase in cyber-attacks. These attacks can result in patient data becoming exposed, healthcare systems 'held hostage' by ransomware hackers, and the health of patients being compromised.

Intertek-EWA Canada has been providing cyber security and assurance testing for critical infrastructure, enterprises. and government agencies for nearly 30 years. Our expertise includes all facets of security assessments, product tests, evaluations, design, and training. We work closely with our customers to provide tailor-made services based on risks factors associated with your specific product. Our offerings are in accordance with guidelines that the FDA has published concerning cyber security recommendations for both premarket submissions and post market management.

Intertek-EWA Canada's cyber security services are a critical component of our full portfolio of IoT solutions which includes software, wireless, conformance and performance testing.

Protecting data whether yours or your customers' is critical. With unparalleled know-how, Intertek-EWA Canada offers a comprehensive suite of security solutions to safeguard data from cyber-attacks.

Regulatory Assurance

Intertek-EWA Canada's IT Security Evaluation & Test (ITSET) Facility is a fully accredited, third-party test facility. We ensure your products and procedures are compliant with the stringent requirements of U.S. and international IT security, information assurance, and data protection standards along with guidelines from the FDA and NIST by providing regulatory assurance for:

- FIPS 140-2
- ISO 15408 (Common Criteria)
- ISO 27001 and ISO 27002 (Evaluations and Trainings)
- Personal Identity Verification

Vulnerability Assessment

Utilizing a thorough and systematic methodology, the vulnerability assessment identifies security issues including any weaknesses in hardware, software, organization, procedures, and personnel. Our experts analyze data, understand the environment in which it operates in, and provide recommendations based on the acceptable risk tolerance. These services include testing of:

- Physical and Digital Security
- Encryption and Authorization Review
- Web, Mobile, and Cloud Interface
- Update and Security Policies

Application Security Penetration Testing

Our security experts conduct white hat testing to actively find breaches through known exploits, verify weaknesses identified in vulnerability testing, and conduct social engineering to identify human risks. These tests are divided into two categories:

- Standard Testing
  - Known Malware/Ransomware
  - Open Web Application Security Project (OWASP) Top 10
- Customized Testing
  - Active Breaching/Hacking
  - Progressive Methodology

Hardware Penetration Testing

Leveraging expertise demonstrated through high assurance testing for the telecom industry, we provide in-depth security analysis of the firmware and hardware of products, infrastructure, and systems including:

- Firmware Source Code
- Operational Firmware Down to Bit Level
- Board Design
- Ports of Entry
- Conformance to Specifications

Data Inspection

Ensuring that data sent is the same data received is critical for any computerized network. Our inspection will prevent unintentional changes to your data and safeguard your systems from intentional attacks by focusing on:

- Data Integrity
- Networks, Systems and Applications
- Supporting Legal and Regulatory Requirements

To learn more about Intertek's medical device services, visit www.intertek.com/medical, call 1-800-967-5352 or email icenter@intertek.com