Healthcare wearables and data security

Consumer wearables collect health-related biometric and behavioural data:

- Exercise data
- Blood pressure
- Glucose levels
- Heart rate
- Sleep patterns
- Menstrual cycles

They also collect personal identifiable information:

- Date of birth
- Geolocation
- IP addresses
- Login details

These devices can expose users to privacy and security risks. Data is often synchronized apps on other devices and is transmitted and stored in cloud-based platforms.

Risks

Malware
Activated by clicking fraudulent links triggering viruses, worms, trojans, spyware, etc. which can delete files and steal information.

Phishing
Deceptive emails or fake websites trick individuals into providing sensitive information, enabling access to personal and health-related data.

Ransomware
Software that encrypts data to prevent user access until a ransom is paid. Attackers can use blackmail – threatening to publish sensitive or valuable personal data.

Distributed Denial of Service attacks
Multiple computers or devices are compromised, then used to attack a target website, service, or app. The target system is bombarded with messages and connection requests.

Manipulation of health data
Wearables are part of an ecosystem with health data being stored on devices, apps, linked phones and computers, and transmitted across Bluetooth and Wi-Fi to cloud-based platforms. Security weaknesses in any area can allow data to be accessed or stolen.

Defence measures

Make device and digital infrastructure secure

Wearables must be secure by design and default. Default settings must be as secure as possible, and security or cryptographic primitives built into hardware and software. Manufacturers must manage device vulnerabilities throughout the product life and develop software patches to address them. Ecosystem and data chains must be secure and constantly monitored.

Make clear and robust data privacy policies

Manufacturers need clear data privacy policies to ensure security and privacy of sensitive health data – not only to comply with data protection legislation but also to provide reassurance that user data are well-protected. The amount of personal identifiable information should be minimized by using unique account numbers and allowing pseudonyms.

How BSI can help

Certification does not guarantee compliance, but it does help your organization strive towards it. An independent body like BSI can assess your management systems and provide support. We also help with product certification as well as management systems certification across ISO 27001, ISO 27701, and ISO 27301 standards. We test your wearable device security, which involves penetrating and hacking into them – all to inspire trust in a more resilient world where we can resist threats.

For more information or to get expert advice please contact cyber@bsigroup.com

The need for industry standards in consumer wearables

Most consumer healthcare wearables don't go through the same rigorous regulatory approval process as clinical-grade devices. As the line between wellness wearables and medical devices blurs, the need for industry standards is more urgent than ever.

Clearly defined standards help manufacturers improve their products' security. Meeting standards and achieving certification enables users to confidently share, store and modify personal data safely.

A lack of industry standards for the Internet of Medical Things (IoMT)

Because there are currently no industry wide standards, any product with a serious security vulnerability may pose a threat to the entire network. Collaboratively developing and ensuring standards for connected IoMT devices would eliminate most vulnerabilities.

Building trust through ISO certification

Wearable users need assurance that the manufacturer/service provider has processes in place to protect privacy and security of sensitive health data. All parts of the ecosystem need to trust that their partners are taking industry standard measures to maximize security.

ISO 27001 relates to information security and provides a framework to develop, implement, monitor, review and continuously improve information security management systems. bsigroup.com/en-GB/iso-27001-information-security/

ISO 27701 focuses on improving privacy information management systems. bsigroup.com/en-GB/iso-27701-privacy-information-management/