Your partner
in progress

Cybersecurity for Medical Devices

Best practice guidelines and regulatory requirements

Cybersecurity

ISO 81001-1 defines cybersecurity as “a state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to confidentiality, integrity, and availability are maintained at an acceptable level throughout the life cycle”.

Current pitfalls

Modern medical devices benefit from improved cybersecurity features. However, many legacy devices still in use today, were not designed to bounce current cybersecurity threats and to meet today’s stringent requirements, potentially posing increased risks to patients’ safety.

Manufacturers are required to ensure that medical devices placed on the EU and UK markets meet the new technology challenges related to cybersecurity risks. This best practice guideline allows you to access the reference documentation in order to fulfill the essential requirements for medical devices cybersecurity.

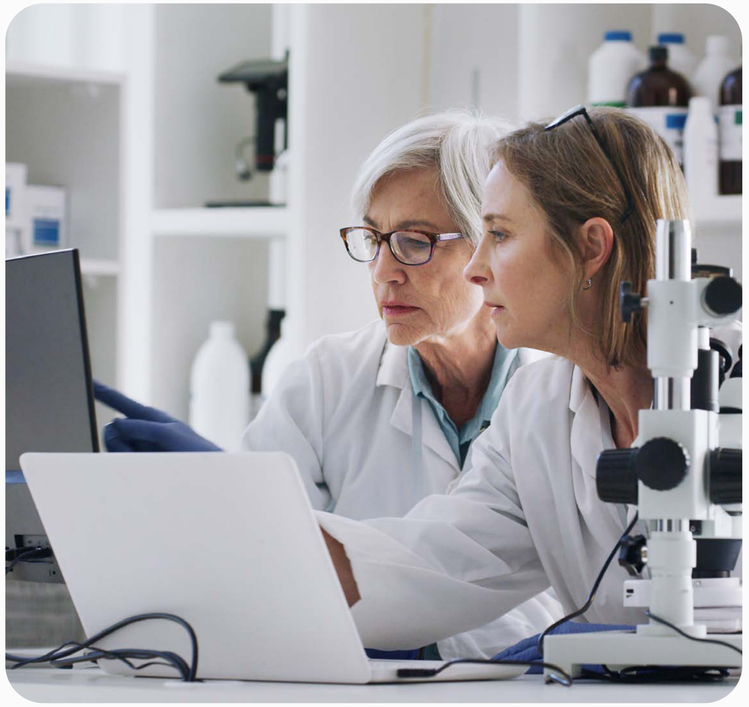
MDR and IVDR requirements

MDR and IVDR introduced stricter safety requirements for all medical devices incorporating electronic programmable systems and software, now considered medical devices themselves. The regulations require manufacturers to develop and manufacture medical devices in accordance with the state of the art taking into account risk management, information security and protection against unauthorized access.

Cybersecurity requirements are listed in Annex I of MDR and IVDR:

- Medical Device Regulation **(MDR) 2017/745**
- In-vitro Diagnostic Regulation **(IVDR) 2017/746**

For additional information on the correspondence of these requirements between the two regulations and on cybersecurity activities to be conducted across the life cycle of medical devices, please refer to **MDCG 2019-16**. For guidance on qualification and classification of software in MDR and IVDR, please refer to **MDCG 2019-11**.



Get in touch

Whether you are starting the certification process, looking to transfer or need to discuss your options, we can guide you through the process.

Request a quote

Other legislation and guidance

Several requirements generally associated with cybersecurity are not explicitly mentioned in the EU MDR and IVDR. Given the growing level of digitalization in healthcare, an increasing amount of national and international requirements and guidance relevant to the domain of cybersecurity are being published.

Europe

NIS Directive
Provides legal measures to improve existing cybersecurity status across the EU through preparedness, cooperation and security culture.

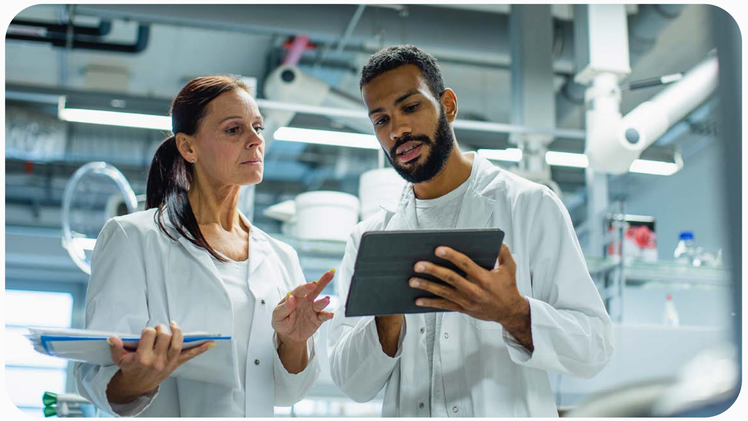
General Data Protection Regulation (GDPR)
Regulates individuals' personal data processing in EU.

TEAM NB on Cybersecurity
Focuses on the harmonization of cybersecurity related Standards, risk assessment, high level penetration test requirements, secure development life cycle and cybersecurity Post-Market Surveillance.

UK

The Data Protection Act 2018 (UK GDPR)
Regulates individuals' personal data processing in the UK.

The NIS Regulation 2018 (UK)
Provides legal measures to improve the level of security of network and information system for the provision of essential and digital services.



International

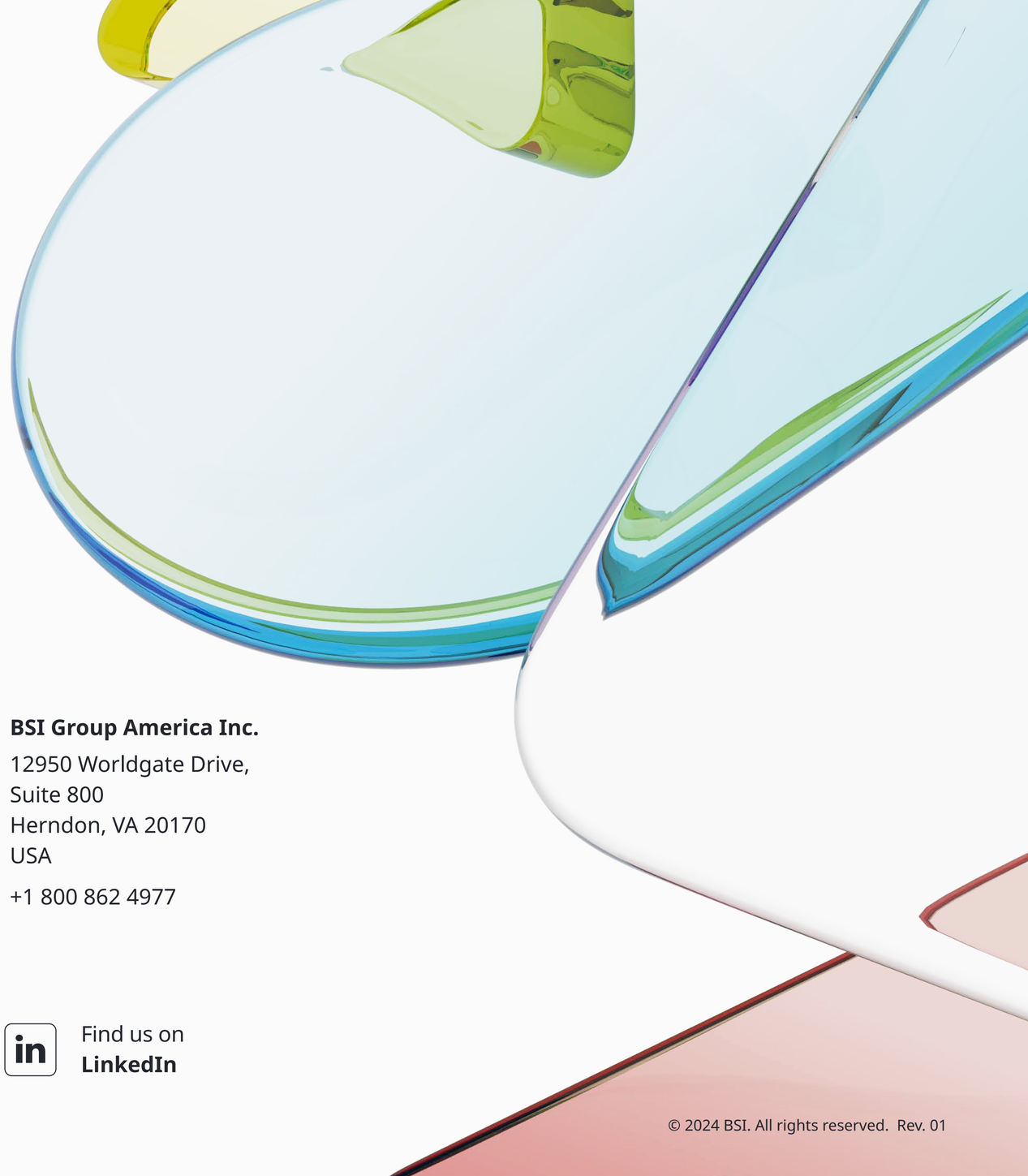
IMDRF Guide on Cybersecurity of medical devices

Complementary to **IMDRF/CYBER WG/N60**, this guide promotes a globally harmonized approach to medical devices cybersecurity. It focuses on foundational security principles and best practices that span the total product life cycle (TPLC) of medical devices.

Risks associated with cybersecurity threats and vulnerabilities should indeed be considered throughout all stages in the life of a medical device, from development through end of support (EOS).

To effectively manage the dynamic nature of cybersecurity risk, risk management should be applied throughout the TPLC where cybersecurity risk is evaluated and mitigated in various parts of the TPLC, including but not limited to design, manufacturing, testing, and post-market monitoring activities.

Your partner in progress



BSI Assurance UK Ltd (0086)

Kitemark Court,
Davy Avenue, Knowlhill,
Milton Keynes, MK5 8PP
United Kingdom

+44 345 080 9000

BSI Group The Netherlands B.V. (2797)

Say Building,
John M. Keynesplein 9
1066 EP Amsterdam
The Netherlands

+31 20 346 0780

BSI Group America Inc.

12950 Worldgate Drive,
Suite 800
Herndon, VA 20170
USA

+1 800 862 4977

Find our services at
bsigroup.com/medical

Email us at
medicaldevices@bsigroup.com

Find us on
LinkedIn