# Medical Device Regulation and Cybersecurity: Achieving 'Secure by Design' for Regulatory Compliance

**William S. ENNS-BRAY, Kim ROCHAT**
Medidee Services SA, Lausanne, Switzerland
william.enns-bray@medidee.com, kim.rochat@medidee.com

**Abstract**

*The rapid evolution of information technology over the past 50 years is transforming our healthcare institutions from paper-based organizations into smart hospitals, a term now used by European Union Agency for Cybersecurity (ENISA). These changes are also associated with the systematic reliance on medical devices by both patients and healthcare providers. While these devices have the potential to advance personalized health solutions and improving the quality and efficacy of care, they nevertheless present significant security risks and challenges throughout the healthcare sector.*

**Index terms:** healthcare, cybersecurity, medical devices, regulations

## References:

[1]. European Union Agency for Cybersecurity. Cybersecurity and resilience for Smart Hospitals. Published November 24, 2016. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals.

[2]. Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication. Published January 23, 2020. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-ge-healthcare-clinical-information-central-stations-and#vulnerabilities.

[3]. Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication. Published June 27, 2019. https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potentialcybersecurity-risks-fda-safety-communication.

[4]. Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication. Published March 21, 2019. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home.

[5]. European Union Agency for Cybersecurity. Defining and securing the Internet of Things: ENISA publishes a study on how to face cyber threats in critical information infrastructures. Published November 20, 2017. https://www.enisa.europa.eu/news/enisa-news/definingand-securing-the-internet-of-things.

[6]. Regulation (EU) 2017/745 of the European parliament and of the council of 5 April 2017 on medical devices.

[7]. MDCG 2019-16 Guidance on Cybersecurity for medical devices. Published December 2019.

[8]. Manufacturer Disclosure Statement for Medical Device Security (MDS2). Published October 8, 2019. https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statementfor-Medical-Device-Security.aspx.

[9]. IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements. Published January 15, 2018.

[10]. IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components. Published February 27, 2019.

[11]. IEC 62304:2006+AMD1:2015 CSV Medical device software – Software life cycle processes. Published June 26, 2015.