January 2023

HOPE Position

on the Cyber Resilience Act

We understand that the proposed Cyber Resilience Act (CRA) Regulation has a horizontal reach and therefore it could be pertinent to various digital networks, IT systems, and Internet of Things (IoT) solutions commonly deployed in hospitals and healthcare environments not covered by other EU legislation. The latter includes, inter alia, the Medical Devices / In Vitro Diagnostic Devices Regulations, the Radio Equipment Directive, the proposed Artificial Intelligence (AI) Act, and the European Health Data Space (EHDS) Regulation proposal with sector-specific measures.

It is well known that the hospital sectors digital infrastructure has been particularly vulnerable to malicious and costly ransomware and other types of cyberattacks in recent years, which have caused a high degree of operational disruption to administration and care while compromising patient safety. Such attacks also threaten the delivery of integrated care strategies comprising multiple health and social interventions to meet complex needs. The proliferation of connected IoT tools in care and domestic settings, and the increased blurring between healthcare and consumer products, further increase the risk of cyberattacks.

From this perspective, the CRA provides a missing link in the expanding EU cybersecurity legislative framework including the recently revised NIHS 2 Directive. It contains harmonised rules for placing connected hard- and software products on the market and for vulnerability handling during the entire product life cycle, coupled with essential cybersecurity requirements for the design and development of products with digital elements. The obligations manufacturers and other supply chain actors will need to comply with are comprehensive and stringent, taking into account cybersecurity risks during all phases between product conception and exploitation.

Put together, the proposed mandatory requirements should enhance the security of many products with digital elements commonly used in hospitals and healthcare, whether generic or tailored, while providing procurers and end users with more transparent information about their cybersecurity properties and safe deployment.

We also note that certain products with digital elements classified as Electronic Health Record (EHR) systems under the proposed EHDS Regulation will need to demonstrate conformity with CRA requirements. While the CRA thus occupies an important role in the EUs cybersecurity architecture, it is nonetheless important to consider that even the very safest products with digital elements, despite having successfully undergone conformity assessment and obtained CE marking, are always subject to interaction with other systems and/or human beings. This interaction could endanger their security, whether deliberately or accidentally; ultimately, it is impossible to safeguard the security of every single interface. However, strong rules are necessary to weave a tight cybersecurity net and, crucially, to protect individuals privacy and personal data, their health and fundamental rights. At the same time, it is important that security properties match users abilities without disturbing service provision.

HOPE feels that further clarification is needed regarding the scope of the CRA and its relevance to everyday hospital and healthcare functions, its relationship with other EU legislation (e.g., to avoid duplication of procedures, but also to ensure that hospitals can continue to work with in-house solutions where necessary), as well as how it relates to developments such as cloud services and open-source software.

As critical infrastructures frequently targeted by cybercriminals, HOPE would appreciate the opportunity to contribute the views and experiences of hospitals and healthcare providers, and help identify relevant vulnerabilities, as part of regular stakeholder dialogues to further improve the EU cybersecurity framework and support the implementation of the CRA.

****

HOPE, the European Hospital and Healthcare Federation, is a European non-profit organisation, created in 1966. HOPE represents national public and private hospitals associations and hospitals owners either federations of local and regional authorities or national health services. Today, HOPE is made up of 36 organisations coming from the 27 Member States of the European Union, as well as from the United Kingdom, Switzerland and Serbia as observer members. HOPE mission is to promote improvements in the health of citizens throughout Europe, high standard of hospital care and to foster efficiency with humanity in the organisation and operation of hospital and healthcare services.