European Healthcare Technology Regulation Briefing | 2025

HEALTHCARE
BUSINESS INTERNATIONAL

Examining Europe's changing healthcare technology regulatory environment for healthcare providers and investors

CONTENTS

PLEASE NOTE THAT THIS EXECUTIVE SUMMARY REPRESENTS A SAMPLE OF OUR FULL REPORT AND SKIPS THE SECTIONS HIGHLIGHTED IN GREY.

HEALTHCARE BUSINESS INTERNATIONAL

EXECUTIVE SUMMARY

The HBI European Healthcare Technology Regulation Briefing provides unique insights into Europe's transforming healthcare technology regulations through 2025, examining four groundbreaking pieces of legislation that will fundamentally reshape the sector.

Drawing on exclusive interviews with senior industry figures, including Harvard professors, multinational law firm partners, and leading health consultants and economists, the report delivers:

• Detailed analysis of the EU AI Act's impact on healthcare technology, including which applications will be classified as "high risk" and practical compliance guidance

• Expert assessment of the European Health Data Space (EHDS) implementation challenges and opportunities

• Critical evaluation of the Cyber Resilience Act's implications for medical device manufacturers, featuring data on healthcare device vulnerabilities

• Strategic insights into the Health Technology Assessment Regulation's harmonisation of clinical evaluations across the EU

The report can help healthcare investors and service leaders to understand how these regulatory changes will affect your business and create new opportunities in the European healthcare technology market.

HBI Intelligence members are able to access the full report. To learn more about Healthcare Business International membership, including HBI Intelligence membership, contact:

Memberships@healthcarebusinessinternational.com
+44 (0) 207 183 3779

INTRODUCTION

The regulatory landscape for healthcare technology is in the process of being drastically altered in Europe. Several major pieces of new regulation have either recently come into force or have been recently approved and are due to come into force soon.

Four pieces of EU-level regulation stand out as being particularly significant for the healthcare sector.

The Health Technology Assessment Regulation (HTAR) came into effect in 2022, but is beginning to be actively implemented in 2025. It aims to strengthen and harmonise the assessment process for new health technologies across EU member states and avoid duplication.

The European Health Data Space (EHDS) is due to begin coming into force in 2025. EHDS aims to remedy the barriers to harnessing healthcare data to improve healthcare delivery and research, especially given GDPR's privacy protections. If successful, it could lead to a more efficient, digitally-integrated healthcare system across Europe and make training new AI models easier.

The EU AI Act, the world's first attempt at a regulatory framework for AI, is set to come into force over 2025–2027. While not healthcare-specific, it will significantly impact the sector. The regulation takes a risk-based approach, with most significant healthcare AI applications likely classed as 'high risk', requiring stringent oversight.

The Cyber Resilience Act, which came into force at the end of 2024, promises to improve the sector's cyber resilience by making it mandatory for med tech manufacturers to implement cybersecurity measures. Healthcare has become one of the most targeted sectors by cyber criminals, with hospitals increasingly aware of vulnerabilities in their systems.

HBI spoke to various legal, health policy and technology experts to get a sense of what impact these changes will have for the sector.

THE CYBER RESILIENCE ACT

Medical device makers must build in security safeguards

- **Act requires manufacturers to submit security plans for all digitally-enabled products**
- **Medical device makers must monitor and patch security vulnerabilities throughout product lifecycle**
- **Rules seem to mirror US approach while offering stronger enforcement, though smaller firms face cost burden**

The Cyber Resilience Act (CRA) is a piece of legislation that imposes cybersecurity regulatory requirements on manufacturers and distributors of any product which has a digital component. Unlike EHDS, it is not specific to healthcare. However, the regulation will apply to all medical device manufacturers.

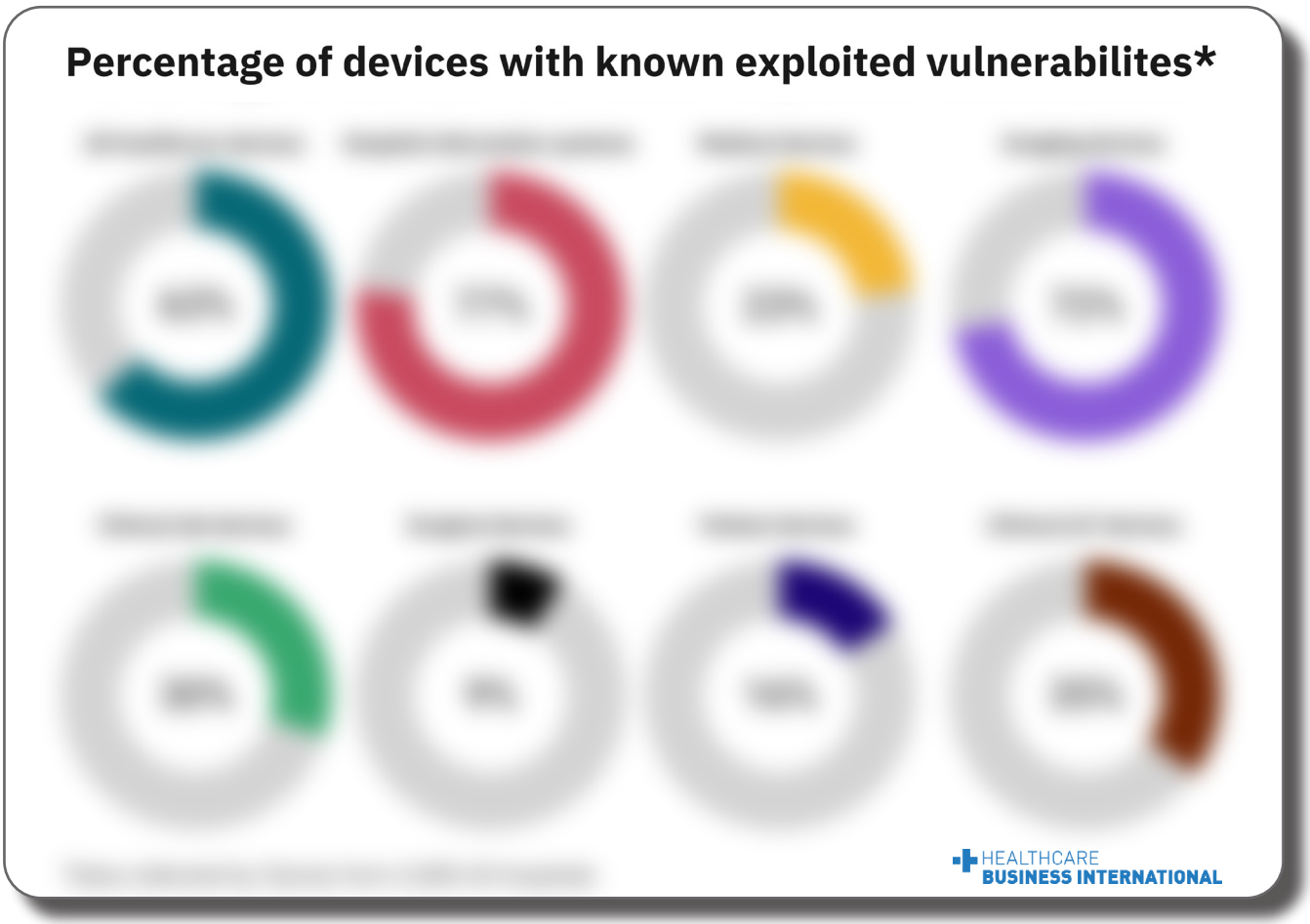
Before going to market, medical device manufacturers will have to submit a plan specifying how they will monitor, identify, and address cybersecurity vulnerabilities on an on-going basis once the product is on the market, and make updates and patches for their devices available.

In effect this means there has to be documentation of a cybersecurity plan for all new devices entering the market.

Ty Greenhalgh, Industry Principal at cyber security solutions provider Claroty, explained that the EU's approach mirrors the approach the US is taking to cyber security in healthcare:

"While the EU Cyber Resilience Act is broader in scope addressing all industries, it is very similar to the approach the US has taken with section 524B of the Federal Food, Drug, and Cosmetic Act (Patch Act), which came into effect in 2023. This gave the FDA teeth to force medical device manufacturers to make their devices more cyber secure. Both pieces of regulation impose a pre-market approval process and post-market evaluation on medical device manufacturers.

"Cyber security in healthcare is



something both Europe and the US have been struggling with for a long time. For years we've had this problem with medical device manufacturers.

"Hospitals have been very upset when they've discovered that by the time the devices they're buying have gone through development and testing, the operating system or some other aspect of the device is out of date. They're buying products that are already legacy products.

"It hasn't been possible to change manufacturers' behaviour through making suggestions and requests. But now that it's becoming a safety issue it is being looked at differently; previously it was looked at as just a data privacy issue."

Greenhalgh told us he believes the EU's approach is superior to the US' approach, because it has breadth across industries and a centralised oversight mechanism, and will therefore be easier to enforce.

"We struggle in the US with fragmented IT systems, and vendors therefore not proactively creating standards because it increases cost, delays time to market and potentially reduces their market share.

"I think the EU will find more success quickly than the US. The EU Cyber

Resilience Act is a good document."

The new cyber security regulation addresses new medical devices entering the market, however it doesn't deal with the millions of legacy devices hospitals already have. But Greenhalgh said the fact that hospitals won't have to worry so much about the new devices they're purchasing will give them more bandwidth to focus on the legacy devices.

"The situation to date has been akin to being in a rowboat and having to continuously bail out water because there is a hole in the boat. Now we've finally had the intelligence to plug the hole, and so we can get rid of the water from the boat instead of forever bailing it out," Greenhalgh said.

As with all stringent regulatory requirements, the CRA will increase barriers to entry to the market, and place a greater burden on smaller and less established firms.

"The EU Cyber Resilience Act will place an additional burden on manufacturers. However, it must be done if we are going to reduce the attack surface of this critical infrastructure. Most manufacturers are selling worldwide, so with the passage of the US Patch Act, they are already required to do this for the US. All the big manufacturers — Philips, Siemens, Fujifilm etc. — are already doing this.

"Is there some relief that could be offered to smaller manufacturers? I don't know."

If these higher barriers to entry make it more difficult to innovate that would be a significant cost of the regulation.

Greenhalgh gave the following example to illustrate the tangible impact these regulations can have, particularly on smaller firms: "There was a smaller US manufacturer that recently went for approval having actively decided they weren't going to consider cybersecurity. It was rejected, and the company had to go back to restart which cost them half a million dollars and almost made them bankrupt. And now that device that could potentially have helped many people is not on the market.

"Regulation for regulation's sake is not good. However, the flip side is lack of resilience to cyberattacks could take down our entire healthcare system, and bleed it dry."

CONTRIBUTORS

PROF. DR. JÖRG DEBATIN
HEALTHCARE CONSULTANT
Independent

MAUREEN DALY
PARTNER
Pinsent Masons

DAVID BATES
PROFESSOR, DEPARTMENT OF HEALTH POLICY AND MANAGEMENT
Harvard University

ERIC SUTHERLAND
SENIOR HEALTH ECONOMIST
OECD

DAVID TALBY
CHIEF TECHNOLOGY OFFICER
John Snow Labs

VINCENZO SALVATORE
HEALTHCARE AND LIFE SCIENCES SECTOR PARTNER
Simmons & Simmons

VE RI TAS
LEX ET IUSTITIA
HARVARD LAW SCHOOL

GLENN COHEN
PROFESSOR OF LAW
Harvard Law School

CLAROTY

TY GREENHALGH
INDUSTRY PRINCIPAL
Claroty

Get in touch

EDITORIAL

REPORT AUTHOR

MARTIN DE BENITO GELLNER
LEAD ANALYST
+44 (0) 204 537 1368

Martin@healthcarebusinessinternational.com

CHRISTOPHER O'DONNELL
HEAD OF CONTENT & EDITORIAL
+44 (0) 204 537 1354

Christopher@healthcarebusinessinternational.com

COMMERCIAL

THOMAS MCMULLEN
MANAGING DIRECTOR
+44 (0) 204 537 1364

Thomas@healthcarebusinessinternational.com

EVENT

LEE MURRAY
EVENTS DIRECTOR
+44 (0) 204 537 1357

Lee@healthcarebusinessinternational.com

Healthcare Europa, operating under the name Healthcare Business International, is a limited liability company registered in England with company number 07823199. The registered office is located at HBI, Commercial Unit A, 111 Seven Sisters Road, London N7 7FN.

HEALTHCARE
BUSINESS INTERNATIONAL

Market Reports are available at
healthcarebusinessinternational.com/intelligence/

For Membership enquiries:

Memberships@healthcarebusinessinternational.com

+44 (0) 207 183 3779