+ *September 2026*

THE CYBERSECURITY WAVE HITTING LIFE SCIENCES AND HEALTHCARE COMPANIES: WHAT YOU NEED TO KNOW

STEPHENSON HARWOOD

Life sciences and healthcare companies – from pharmaceutical manufacturers and medical device makers to hospitals, care providers and digital health platforms – face a rapidly evolving cyber regulatory landscape across the EU and UK. Four major laws could impose significant obligations and carry substantial penalties for your organisation. Here is what you need to know.

EU: CYBER RESILIENCE ACT

What it is

Cyber regulation establishing horizontal cybersecurity requirements for products with digital elements placed on the EU market that connect to another device or network.

Who it might apply to

Connected wellness devices, digital healthcare platforms, connected laboratory and healthcare equipment. This does not include EU MDR-regulated devices.

Key obligations

- Cybersecurity and conformity assessment
- Appoint an authorized representative
- Vulnerability handling throughout the product lifecycle
- Report exploited vulnerabilities (within 24 hours)
- Security updates for min. 5 years

Enforcement

Fines up to €15m or 2.5% of global annual turnover. Non-compliant products may be withdrawn from market.

Vulnerability reporting effective date: Sept 2026
Remaining requirements effective date: Dec 2027

EU: NIS2 DIRECTIVE

What it is

The Network and Information Systems Directive 2, setting out cybersecurity obligations for essential and important entities offering their products and services across the EU.

Who it might apply to

Health sector entities including healthcare providers, pharma manufacturers, certain medical device manufacturers and R&D organisations.

Key obligations

- Registration
- Risk management for network and information systems
- Incident reporting (24h early warning, 72h full notification)
- Supply chain security and business continuity
- Board-level accountability for cybersecurity

Enforcement

Fines up to €10m or 2% of global annual turnover.
Personal liability for management bodies.

Effective date: Oct 2024 (many EU member states have been delayed in implementation)
Entities should be compliant now

UK: CSR(NIS) BILL

What it is

Cyber Security and Resilience (Network and Information Systems) Bill, updating and expanding the existing cybersecurity framework under the NIS Regulations 2018 (NIS) to cover a broader scope of products and services.

Who it might apply to

Relevant managed service providers and operators of essential services (OES) in the health sector, including designated independent healthcare providers, and designated critical suppliers to healthcare OES.

Key obligations

- Registration
- Enhanced risk management duties
- Expanded and faster incident reporting requirements
- Supply chain security obligations
- SoS powers to update regime via secondary legislation

Enforcement

Strengthened regulatory powers and significant penalties. ICO given stronger enforcement tools including proactive investigation.

Royal Assent 2026. Secondary legislation and guidance to follow — prepare now

UK: PSTIA

What it is

Product Security and Telecommunications Infrastructure Act setting out provisions about the cybersecurity of internet-connectable products made available to consumers in the UK.

Who it might apply to

Connected wellness devices and other connected consumer products. This does not include UK MDR-regulated devices.

Key obligations

- Adopt specified security requirements
- Issue a statement of compliance with product
- Investigate and act in the event of a compliance failure
- Compliance failure reporting to authorities and to consumers (as soon as possible)
- SoS powers to update regime via secondary legislation

Enforcement

Fines up to £10m or 4% global annual turnover. Secretary of State has the power to order changes to cybersecurity measures and to recall a product.

Effective date: 6 Dec 2022
Entities should be compliant now

These laws carry significant penalties and require action now. Contact our Cyber team to discuss how these obligations apply to your organisation.

Please note: this alert highlights four key cyber security laws but is not an exhaustive list of all legislation that may apply to your organisation.

YOUR CYBER KEY CONTACTS

JOANNE ELIELI
Partner, Cyber Lead
+44 20 7809 2594
+44 7386 688752
Joanne.Elieli@stephensonharwood.com

SARAH O'BRIEN
Partner
+44 20 7809 2481
+44 7766 828548
Sarah.Obrien@stephensonharwood.com

ALISON LLEWELLYN
Senior Knowledge Development Lawyer
+44 20 7809 2278
+44 7557 162343
Alison.Llewellyn@stephensonharwood.com

YOUR LIFE SCIENCES AND HEALTHCARE KEY CONTACTS

ALEXANDRA PYGALL
Partner - Head of Life Sciences & Healthcare
+44 20 7809 2137
+44 7881 314566
Alexandra.Pygall@stephensonharwood.com

DAN HOLLAND
Partner
+44 20 7809 2108
+44 7841 923656
Dan.Holland@stephensonharwood.com

NAOMI LEACH
Partner
+44 20 7809 2960
+44 7769 143367
Naomi.Leach@stephensonharwood.com

+ A LEADING PRACTICE

Our Cyber team brings deep expertise across all aspects of cyber security, helping clients stay ahead of shifting legal frameworks while safeguarding their operations. We support clients with comprehensive advice on the full spectrum of:

Preparation and prevention: cyber advisory and compliance, corporate transactions, audits and investigations support; and incident response planning.

Containment, eradication and recovery: responding to cyber incidents (including ransomware attacks, nation-state espionage, business-email compromise fraud, phishing attacks, insider incidents, 'bad leaver' security issues and social engineering attacks); and crisis management.

Post-incident activity: investigations (regulatory and internal); high-stakes, complex cyber disputes; and post-incident analysis.

STEPHENSON HARWOOD

*"Great, friendly, approachable team. **Extremely efficient** in coming back with their work. **Very practical**, business-friendly advice."*

*"A team of highly knowledgeable experts in their field, **providing practical, no-nonsense advice with a pragmatic focus.** They quickly seek to understand the issues and provide clear direction informed by their strong links with the regulator."*

THE LEGAL 500 UK 2026, DATA PROTECTION,PRIVACY & CYBERSECURITY

*"They truly **understand how we operate** as a business, **what our risk appetite is**, who our consumers are and the goals we have for the business."*

CHAMBERS UK 2026, DATA PROTECTION & INFORMATION LAW

PICCASO AWARDS EUROPE

*PICCASO Privacy Awards 2025 – awarded **'Law Firm of the Year'***