Regulating medical device cybersecurity risk by the U.S Food and Drug Administration(FDA)

By: Andy Watkin-Child & Jamie Foster

March 2023

THE AUGUSTA GROUP

HILL DICKINSON

Introduction

Cyber risk regulation is quickly developing in the U.S and EU, regulations that have a significant effect on the pharmaceutical industry and medical device manufacturers. Requiring increased disclosure of material cyber risks, material cyber incidents, the role of the board in cyber risk oversight, assurance and attestation, the implementation of cybersecurity risk management, cybersecurity programs, the disclosure of cyber incidents and the knowledge and experience of management and accountable executives in cybersecurity risk management oversight and assurance. These regulations transfer cyber risk management into the board rooms of covered entities, increasing corporate legal and compliance risks and exposing Directors, Officers and accountable executives to increased personal legal risks. As insurers move to clarify D&O and cyber insurance coverage for regulatory breaches.

Reliance on digital infrastructure creates cyber risks for all organisations, and for those operating in the healthcare sector this includes the risk inherent in medical devices which rely on software. U.S regulators passed a law requiring medical devices to meet cyber security standards for FDA authorisation, and the EU and UK are moving in the same direction.

The US 2023 Consolidated Appropriations Act signed into law device medical cybersecurity

On the 29th of December 2022, the U.S President signed into law the 'Consolidated Appropriations Act 2023[1]'. This is the Omnibus spend that packages smaller appropriation bills into a single larger bill that can be passed by U.S Congress. The Act signed into law $1.7 trillion to fund U.S federal Government for 2023, apportioning spending across a wide range of Federal activities and laws.

The Act is a significant document that funds federal agencies, departments and administrations that includes the Food and Drug Administration (FDA) for the forthcoming year. It has also been known to pass regulations and laws, and the 2023 Consolidated Appropriation Act was no exception. Under 'TITLE III - *FOOD AND DRUG ADMINISTRATION*, *Subtitle C – Medical devices*', a requirement for '*ENSURING CYBERSECURITY OF MEDICAL DEVICES)'* was signed into law (SEC 3305*)* which is effective from the 29th of March 2023[2], 90 days from the enactment of the Act.

The requirement applies to medical device manufacturers who submit device applications to the FDA under section 510(k), 513, 515(c), 515(f), or 520(m) and meet the definition of a 'cyber device', meaning devices that have software installed; have the ability to connect to the internet and have technical characteristics that could result in a vulnerability to cybersecurity threats. Where this is the case the manufacturer or sponsor of an application must.

- Submit a plan as to how they will monitor, identify, and address as appropriate, in a reasonable time, post market cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures.

[1] https://www.appropriations.senate.gov/imo/media/doc/JRQ121922.PDF
[2] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-refuse-accept-policy-cyber-devices-and-related-systems-under-section#:~:text=The%20Omnibus%20states%20that%20the,)%20before%20March%2029%2C%202023.

- Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure. By making available post market updates and patches to the device and related systems to address known unacceptable vulnerabilities, and critical vulnerabilities that could cause uncontrolled risks.
- Provide a software bill of materials (SBoM), including commercial, open-source, and off-the-shelf software components.
- Comply with such other requirements as the FDA may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

This is a significant development for medical device manufacturers globally. It opens the way for the FDA to mandate cybersecurity risk management of medical devices that includes vulnerability and patch management, the management of the Software Development Lifecycle and attestation over product cybersecurity.

The position in the U.S, EU and UK

The FDA requirement comes at a time when regulators are introducing cybersecurity risk management regulation globally. European Union released the EU NIS 2 directive (EU 2022/2555[3]) on the EU Journal in January 2023, to be transposed by EU Member States by October 2024. EU NIS 2.0 affects Critical National Infrastructure (CNI) providers. Providers that include those from the health sector and the manufacturers of medical devices, considered to be critical during a public health emergency under Article 22 of regulation (EU) 2022/123[4]. EU NIS 2 requires the management bodies of CNI providers to implement cybersecurity risk management processes, practices, measures, and risk mitigation, undergo risk-based *ex-ante* and *ex-post* supervision, report significant cyber events to the National CSIRTs within 24 hours and deliver management and corporate cybersecurity education programs.

On the 1st of March 2023 the U.S president signed the National cybersecurity strategy[5]. That formalises U.S cybersecurity strategy by the Executive Office. Laying out for example further cybersecurity regulation that will affect Critical National Infrastructure(CNI) providers, including the healthcare sector.

The U.S Securities and Exchange Commission(SEC) finalised cybersecurity risk management regulation[6], effective 5th September 2023 and affects public firms covered under the Securities and Exchange Act 1934. That includes registrants across the U.S and EU pharmaceutical sector, requiring the reporting of material cyber risks, material cyber incidents, disclosure of the role of the board in cyber risk oversight, assurance and attestation, the implementation of cybersecurity risk management, cybersecurity programs, the disclosure of cyber incidents and the knowledge and

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0123
[5] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/
[6] https://www.sec.gov/news/press-release/2023-139

experience of management and accountable executives in cybersecurity risk management oversight and assurance, and is a further sign that cybersecurity regulation is being taken seriously.

While in the UK it remains to be seen how the government will implement the outcome of its consultation on proposals to improve the UK's cyber resilience, including by updating the current Network and Information Systems Regulations 2018 (SI 2018/506) (NIS Regulations), steps are being taken towards regulating cybersecurity risk in medical devices. The government proposes to include cybersecurity as an essential minimum requirement for software as medical devices. This proposal arises from a consultation on future regulation carried out in 2021, in response to which industry broadly welcomed the introduction of cybersecurity requirements and recommended alignment with international frameworks and standards. As a result, the government intends to introduce a requirement akin to EU MDR General Safety and Performance Requirement (GSPR) 17.4 (for medical devices) and EU IVDR GSPR 16.4 (for IVDs) covering cybersecurity and associated requirements. And building on this, the MHRA's Software and AI as a Medical Device Change Programme, includes mitigating cybersecurity risks as one of its work packages.

Conclusion

Cyber regulation that affects the pharmaceutical industry and medical device manufacturers is now effective. The SEC released the cyber final rule requiring cyber reporting through 8K and 10K forms, informing market participants that includes investors, of the cybersecurity posture of registrants. EU NIS 2 will affect the pharmaceutical sector and medical device manufacturers from October 2024. The FDA requirement is a further piece of cybersecurity regulation that requires medical device manufacturers to submit a plan to monitor, identify, and address, as appropriate, in a reasonable time, post market cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures; Design, develop, and maintain processes and procedures to provide a reasonable assurance that devices and related systems are cybersecure, and make available post market updates and patches to the device and related systems to address; Provide a software bill of materials, including commercial, open-source, and off-the-shelf software components, amongst other things. Irrespective of the size of the organisation if device manufacturers want to sell their products or services into the U.S, they are required to comply with FDA device cybersecurity requirements.

The medical device industry is facing cybersecurity risk regulation and requires adapting to provide oversight, assurance and attestation of cybersecurity risks. For some, adapting to regulation across several jurisdictions.