ICLG

The International Comparative Legal Guide to:

Cybersecurity 2019

2nd Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Angara Abello Concepcion Regala & Cruz Law Offices
Bagus Enrico & Partners
Boga & Associates
BTG Legal
Christopher & Lee Ong
Cliffe Dekker Hofmeyr Inc
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Ferchiou & Associés
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
JIPYONG LLC
King & Wood Mallesons
Latham & Watkins LLP
Lee, Tsai & Partners Attorneys-at-Law
LT42 – The Legal Tech Company
Maples and Calder
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Simmons & Simmons LLP
Siqueira Castro Advogados
Stehlin & Associes
Synch
Templars
USCOV | Attorneys at Law

glg
global legal group

glg
global legal group

Contributing Editors
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Sam Friend

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
October 2018

ISBN 978-1-912509-38-6
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Cybersecurity and Digital Health: *Diabolus ex Machina*?

Paolo Caldato

David Fitzpatrick

Simmons & Simmons LLP

1 Introduction

In July 2018, Singapore experienced its most severe cyber-attack to date. Hackers targeted the city-state's largest healthcare group, copying the personal data of 1.5 million patients[1] and leaking the details of medicine dispensed to about 160,000 people, including the Prime Minister.[2] While few attacks have taken place on such a grand scale, this is by no means an isolated incident, and the evidence suggests that the incidence of further attacks on the healthcare industry will accelerate.[3]

The adoption by healthcare organisations and consumers of the Internet of Things, cloud-based services and "big data" analytics is now the norm.[4] A key feature of this new landscape has been the explosion of mHealth apps and other digital health technologies on the market (and in the pipeline). These products push the boundaries of innovation, and enable an enhanced and more efficient healthcare delivery service that does not operate exclusively within large healthcare organisations but is available at consumers' fingertips. This promises to transform and disrupt how consumers access medical services and receive (and take responsibility for) bespoke healthcare in the developed world, and has already allowed medical technology to leap-frog traditional infrastructure challenges in Africa.

Digital health has also revolutionised the collection and processing of personal medical data, particularly in terms of the categories and volumes of data being collected. The analytical possibilities offered by the availability of these data, and their consequent socio-medical applications, are endless and promise very real opportunities for consumers to receive personalised, real-time healthcare services that could materially reduce the cost for national health services of treating chronic and lifestyle diseases and associated medical complications.

However, with the increased availability of data comes both increased interest in stealing those data and increased vulnerability to attempts to do so. Despite the pressing need for effective defences against cybersecurity breaches, many of these innovations are not sufficiently well-equipped to withstand the tide of attacks on the horizon; in many cases, the issue of cybersecurity is relegated to an afterthought. This has led to medical devices (including digital health technology) being described as "the next security nightmare".[5]

In order to play catch-up with this new technological reality, the European Union has introduced a raft of new regulation over the past two years. In reality, much of this is intended to address other subjects, and at times, references to cybersecurity remain few and far between, and difficult to pinpoint. That said, it is undeniable that the regulatory burden on companies engaged in digital health has increased, and will continue to do so; in this respect, neglect of cybersecurity goes far beyond a major hindrance to service delivery, but can be the catalyst for potentially crippling fines, unwelcome litigation and, ultimately, reputational meltdown.

These difficulties can leave potential investors in these technologies with a headache: any up-side in investing will not be predicated solely on product quality or innovation, but also on the robustness of the company commercialising the product or innovation in question, and its ability to prevent, and (perhaps more realistically) reduce the impact of, cybersecurity incidents.

2 The Vulnerability of Medical Devices

Digital health technology has rapidly evolved in recent years: non-networked and isolated equipment has quickly made way for fully-fledged networked equipment with features such as remote access, wireless connectivity and pre-installed software, used widely both within healthcare organisations and by consumers at home. Often, this technology is connected to smart devices, such as mobile phones and tablets. Wearable devices incorporating medical apps and software are also on the rise. Increasingly, these products require personal data to function. However, vulnerabilities are not limited to data leaks; in the most extreme cases, hacks can give access to other networks, install ransomware or achieve control of the device itself.

These concerns have played out in practice and have the potential to be life-threatening. In October 2016, Johnson & Johnson warned its patients that a security vulnerability in its networked insulin pumps could potentially enable hackers to administer insulin overdoses to diabetic users.[6] In August 2017, around 465,000 of St Jude Medical's pacemakers were recalled by the U.S. Food and Drug Administration (the "FDA") owing to concerns over their connections to mobile devices and diagnostic systems that left them vulnerable to tampering.[7] Such concerns were not lost on former U.S. Vice President, Dick Cheney, who asked that his doctors modify his heart defibrillator so as to thwart its vulnerability to hacking.[8]

Often, it is not large, established organisations well-versed in risk and regulation that are behind these products. Instead, they are frequently conceived, marketed and supported by start-ups, who may be tempted (or financially compelled) to forgo the integration of security mechanisms in order to expedite the launch of their products onto a fast-moving market. Although coding errors, insecure protocols, out-of-date software and password flaws remain possible, product quality and associated patient care issues, rather than security, are likely to be their primary concerns. This is reflected in much of the regulation that governs medical devices, which contains no shortage of information on matters concerning patient health, but offers sparse detail to address the prevention, and remediation, of cybersecurity breaches.

Clearly, these difficulties present fertile ground for hackers, who employ all manner of tactics, such as spoofing or impersonation, social engineering, phishing, and malicious code, in order to compromise medical devices. A current phenomenon is the use by criminals of malware to encrypt information before demanding payment via digital currency to recover the information (including patient records). And, of course, there is always the risk of a data breach being committed by a disgruntled employee with access to sensitive information.

3 Regulatory Framework

The regulatory framework that governs the security of medical devices in the European Union is patchwork in nature and lags behind the US regime, where the FDA has issued several pieces of guidance on the issue that directly address cybersecurity.[9] This disparity is, in no small part, due to the fact that current European regulations tend to focus on patient safety but contain very few direct references to cybersecurity risk. Furthermore, no single set of standards can be found in one place, but must be filtered through three separate lenses: (i) regulations in relation to medical devices; (ii) cybersecurity-specific regulation; and (iii) data protection regulation. Cognisant of the need for regulation to catch up with the exponential increase in new technologies, the EU has been legislating in each of these three fields. As a result, cybersecurity can no longer tenably be considered an issue that permits a reactive approach; instead proactive engagement will be required from stakeholders throughout a product's supply chain and lifespan.

Medical Devices Regulation

The European Parliament recently conducted a comprehensive revision of European legislation of medical devices, pursuant to which, amongst other things, the Medical Devices Directive[10] and the Active Implantable Medical Devices Directive[11] are being phased out and replaced by a new Medical Devices Regulation (the "MDR").[12] The MDR entered into force on 25 May 2017, with a transitional period of three years.[13]

The Medical Devices Directive, as amended, already confirmed that software in its own right can fall under the definition of medical device, where the software is intended by the manufacturer to be used for the purpose of:

(i) diagnosis, prevention, monitoring, treatment or alleviation of disease;

(ii) diagnosis, monitoring, treatment, alleviation or compensation for an injury or handicap;

(iii) investigation, replacement or modification of the anatomy or of a physiological process; or

(iv) control of conception.

The MDR expands this definition to include devices used for the "prognosis" and "prediction" of diseases[14] and, by association, their accessories (that is, articles intended by manufacturers to be used in accordance with the device's purpose or to assist its functionality).[15] A list of product groups that, despite having no intended medical purpose (notably, products introduced into the body via surgically invasive means in order to modify anatomy, and equipment using electrical or magnetic currents to stimulate the brain) will also be treated as medical devices,[16] and the European Commission has reserved the right to add new groups by means of delegated acts.[17] However, the MDR stops short of including in the definition software intended for general purposes, such as lifestyle and well-being apps. While there are sure to be grey areas, this broader definition presents challenges for an exponentially growing market; what a manufacturer may consider to be the latest home-health gadget could actually transpire to be a medical device that requires strict regulatory compliance (including in relation to cybersecurity) in order to be commercialised legally.

The MDR goes further than previous legislation in its explicit reference to cybersecurity. It requires devices to be designed and manufactured in such a way as to: (i) remove or reduce as far as possible the risks associated with the possible negative interaction between software and the IT environment with which it operates and interacts;[18] and (ii) protect against unauthorised access that could hamper the device from functioning as intended.[19] Manufacturers are also required to set out minimum requirements concerning hardware, IT network characteristics and IT security measures, including protection against unauthorised access.[20]

General Data Protection Regulation

The General Data Protection Regulation (the "GDPR"),[21] which came into force on 25 May 2018 and is supplemented in the UK by the Data Protection Act 2018 (the "DPA"),[22] requires data controllers to comply with six data protection principles[23] with respect to personal data (a broad concept that encompasses any information, including health data, that can be used to identify an individual).[24] The sixth data principle states:

> "*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures.*"[25]

While much GDPR-related discussion in the healthcare industry has centred on the issues of the collection, storage and use of patient data, and associated consent, the GDPR increases the demands on healthcare organisations and app developers from a cybersecurity perspective: both data controllers *and* processors are required to implement security measures that are appropriate, taking into account factors such as data type, the nature and purpose of processing, the risk to individual rights associated with any security breach and the costs of implementation.[26] The following examples are given in the legislation: (i) anonymisation (or "pseudonymisation")[27] and encryption; (ii) ensuring the ongoing confidentiality, integrity, availability and resilience of the systems that process the data; (iii) the ability to restore access in a timely manner following an incident; and (iv) a process to test, access and evaluate the effectiveness of those security measures.[28]

Personal data breaches must be notified by data processors to data controllers, and by data controllers to the relevant supervisory authority (in the UK, the Information Commissioner's Office (the "ICO")) without undue delay.[29] In the case of data controllers, this notification should, where feasible, take place within 72 hours of the data controller becoming aware of the breach, but no notification need take place if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.[30] Where such a risk is high, however, the data controller must, without undue delay, notify the data subjects of the personal data breach, unless: (i) appropriate technical and organisational protection measures were applied to the data affected by the breach; (ii) the data controller has taken subsequent measures to ensure that the risk to rights and freedoms of data subjects is no longer likely to materialise; and (iii) it would involve disproportionate effort (in which case, there would instead be a public communication or similar measure whereby the data subjects would be informed in an equally effective manner as that prescribed by the notification requirements).[31] Breaches are not to be taken lightly and can lead to fines of up to 4% of global annual turnover.[32]

NIS Directive

Comparatively little attention has been given to the EU Directive on the Security of Networks and Information Systems (the "NIS Directive"),[33] which is often referred to as "the Cybersecurity Directive". The NIS Directive was implemented in the UK on 10 May 2018 by the Network and Information Systems Regulations 2018 (the "NIS Regulations"). The NIS Directive subjects operators of essential services ("OESs"), such as healthcare providers, and relevant digital service providers ("RDSPs"), including cloud computing services, to additional risk management and reporting requirements.[34] A myriad of medical devices and digital health apps fall under the scope of the NIS Directive by virtue of constituting network and information systems under the terms of the legislation.[35]

In the UK, the NIS Regulations favour broad outcome-based principles over prescriptive rules. The National Cyber Security Centre (the "NCSC") has published four top-level objectives for OESs (under which sit 14 high-level compliance principles). These are: (i) managing security risk; (ii) defending systems against cyber-attacks; (iii) detecting cybersecurity events; and (iv) minimising the impact of cybersecurity incidents.

OESs are required to report any incident that "has a significant impact on the continuity of the essential service which that OES provides",[36] while RDSPs must report "any incident having a substantial impact on the provision of any of the digital services [that applies]".[37] Reporting timeframes mirror those in the GDPR, in that notification to the relevant competent authority[38] must take place "without undue delay" and no later than 72 hours after the OES or RDSP becomes aware of the incident.[39] Relevant competent authorities are empowered to monitor compliance with security and notification duties by conducting, or ordering, inspections (the reasonable costs of which will be borne by the relevant OES or RSDP).[40] The most serious breaches of the NIS Regulations can leave a company liable for a fine of £17,000,000.[41]

Although the NIS Directive and the GDPR are products of different EU concerns (the former is intended primarily for companies that are involved in providing critical infrastructure services, while the latter addresses all organisations that process personal data) there is a considerable degree of overlap between the Regulations as they pertain to cybersecurity. For example, if a digital health provider or healthcare organisation were hacked, both the personal data that it holds (in respect of which the GDPR would apply) and its service delivery (in respect of which the NIS Directive would apply) would likely be compromised.

4 Breach and Liability

A business that has fallen victim to a cybersecurity breach will have to invest substantial sums in internal remediation measures, which will require a full exploration of the breach, as well as of the proposed measures to contain, and eradicate, the threat and the steps to ensure that the system is future-proofed against similar attacks. However, a breach can have an impact far beyond the immediate aftermath and remediation process: large regulatory fines, litigation and reputational damage are very real prospects. It is, therefore, important for investors to consider these risks and assess where liability may lie in the event of a breach.

ICO fines

The ICO has had the power to issue fines for failures to follow security obligations from as early as 2010. These fines were linked regularly to breaches of the seventh data protection principle (often in connection with other principles) under the Data Protection Act 1998,[42] the wording of which (much like that in the GDPR's sixth principle) required:

> *"…appropriate technical and organisational measures… against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

For example, in February 2017, the ICO fined private health company, HCA International Ltd, £200,000 for its failure to safeguard the confidential personal information of fertility patients.[43]

It remains to be seen how enforcement action will look in the post-GDPR climate. The severity of the sanctions now available to the ICO, coupled with an increase in the ICO budget for 2018/2019 from £24 million to £34 million (partly owing to the need for more enforcement officers),[44] might suggest that higher fines will become the norm. Indeed, in one of its first instances of enforcement action following the entry into force of the GDPR, the ICO penalised Facebook with the maximum available fine under the Data Protection Act 1998 of £500,000 (and noted that the sum would have been more hard-hitting had the breaches occurred after the commencement of the GDPR on 25 May 2018) for the social media titan's role in the Cambridge Analytica scandal, which resulted in the harvesting of, allegedly, 50,000,000 user profiles. Some experts consider this to be a warning shot from the ICO and an indication that future enforcement action will have more teeth than previously was the case.[45] Such assertions may, however, be premature: the ICO has indicated that it has "no intention of changing the ICO's proportionate and pragmatic approach" and that "hefty fines will be reserved for those organisations that persistently, deliberately or negligently flout the law". Whichever view one takes, the digital health industry should pay particular attention to the ICO's intended focus on large-scale data and cybersecurity breaches involving sensitive information.[46]

Civil litigation

Irrespective of whether or not regulatory action has been taken, digital health companies remain vulnerable to court claims as a result of cybersecurity attacks involving their products. Under English law, claims may be brought pursuant to various causes of action, such as: (i) tortious misuse of private information; (ii) tortious or contractual breach of confidence; (iii) breach of a contractual term (express or implied) that customer data will be stored securely and with due care; (iv) tortious or contractual negligence, for a failure to take reasonable security precautions when storing customer information; and (v) under Article 82 of the GDPR for damage caused by a breach of the GDPR, and/or under section 169 of the DPA for a breach of data protection legislation, in the form of a compensation claim against the defendant data controller and/or processor.

Traditionally, UK cybersecurity cases have occupied little court time, largely owing to the uncertainty surrounding whether or not individuals have suffered damage (and, if so, how to quantify it). Claims made, or threatened, against businesses for a breach of the Data Protection Act 1998 were often low-value, and alleged offenders tended to opt for confidential settlements over the prospect of a PR disaster.

The GDPR may signal the dawn of a more litigious culture in healthcare, at least in relation to breaches involving personal data. Whereas previously, consumers may have been kept in the dark as to a breach, the new self-reporting requirements mean that they will now be notified of a breach at the same time as the regulatory authority; large regulatory fines may encourage "knock-on" litigation (or even motivate particularly vexed consumers to bring claims during the ICO's enforcement process).

Prohibitively expensive claims may also become less of an issue: data subjects are now entitled to appoint certain non-profit bodies to lodge a complaint on their behalf and exercise their right to compensation,[47] which could enable groups of claimants to be brought together through, for example, group litigation orders. Although the GDPR is very much in its infancy, it is not difficult to imagine opportunistic claims management companies heavily advertising the possibility of knock-on litigation following major data breaches. Furthermore, whilst pecuniary loss was formerly a prerequisite, the GDPR confirms the Court of Appeal's decision in *Vidal-Hall et al v Google*[48] that "damage" caused to consumers by data controllers and processors can include emotional distress alone; the terminology used in the GDPR is "material" or "non-material" damage.[49]

Contracts may also provide a basis for further liability in the event that a business's cybersecurity systems are compromised, although the relevant contractual nexus (and therefore, where that liability lies) will be heavily dependent on the way in which the product is delivered to, and operated in, the market. Where digital health companies not only design and manufacture products, but also support or run those products as third-party service providers for healthcare organisations, they may face claims for termination or contractual damages, pursuant to data protection clauses that have been breached as a result of cybersecurity failures. Consideration should also be given to any misrepresentations made to healthcare organisations, direct customers, or other third parties, as to the robustness of the app's cybersecurity systems. Such statements may have made their way into, for example, responses to RFPs, or prospectuses or marketing materials (as well as, of course, contractual documentation), and could result in misrepresentation claims by shareholders, suppliers, customers, or even investors.

Irrespective of whether or not the cybersecurity incident in question causes a data breach, in the absence of enforceable contractual restrictions on liability, claims can arise where the disruption to a business caused by a cybersecurity incident leaves the business unable to fulfil other contractual duties owed to its business counterparts.

Investors considering board seats after the acquisition of a digital health company should also be aware that they themselves may be potentially exposed to creative consumer claims, most likely for alleged breaches of fiduciary duties under the Companies Act 2006. Attempts could be made, for example, to argue that a failure to mitigate, and remedy, a cybersecurity incident constitutes a breach of a director's duty to promote the success of the company,[50] and/or to exercise reasonable skill and diligence in the conduct of his role, which, if made out, could give rise to personal liability on the part of the director.[51] Furthermore, and although it is no easy task to pierce the corporate veil and establish personal liability, that same creative claimant might attempt to fix a shareholder that was not on the board but was nonetheless active in the management of (or could be shown to be particularly knowledgeable about the business of) the digital health company with liability in respect of any such consumer claim.

Even if litigation does not materialise, where customer data have been compromised, companies can find themselves feeling pressure to offer to their customers significant *ex gratia* goodwill payments in order to mitigate any damage that the breach has caused to the customer relationship. And, of course, additional pressure to reach such an accommodation (on a confidential basis) is likely to arise from the fact that consumers (particularly those within patient groups) are heavily active on social media, and awareness of a successful claim is consequently likely to spread rapidly (and thereby generate copy-cat claims).

Whatever the nature and basis of a potential dispute, investors should be live to the fact that litigation is uncertain, and even where claims asserted are meritless, they still require time and money to be properly defended, and can lead to the business in question being irreparably damaged from a PR perspective.

5 Practicalities

Any consideration of an investment in a digital health entrepreneur should not be predicated solely on product quality. The investment decision should be influenced by a deep understanding of the business through which it is commercialised, or supplied to consumers or healthcare organisations. Ultimately, even the most innovative product on the market is likely to fail (and destroy any investment value) if it is commercialised in a way that leaves it vulnerable to significant losses, including through a failure to pay due regard to cybersecurity and the consequences of a data breach. The principal means of mitigating against this is proper due diligence, including a thorough understanding of the technology's genesis, purpose and method of operation, and an assessment of the business's ability to meet the regulatory requirements outlined above.

There is no shortage of resources available for those trying to navigate the complex issues that cybersecurity threats pose to investment in this sphere. Various guidance has been published by organisations such as the NCSC[52] and the British Standards Institution, the latter of which has published a paper that directly addresses the cybersecurity of medical devices.[53] Lessons can also be taken from the more developed US model.

As a guide, we set out below a (by no means exhaustive) checklist of relevant overarching considerations, divided into four categories: (i) risk assessment; (ii) contract; (iii) business culture; and (iv) incident response. It seems likely that, owing to the nature of digital health entrepreneurs, investors will have to be prepared to bring to the table ready-made solutions to these issues, rather than expecting a small digital health company with little experience, manpower or interest in commercial matters beyond innovation, to be market-ready on its own. Investors should, as with any potential investment, exercise a healthy sense of scepticism when weighing the opportunity, and should not be distracted from detailed enquiries by, for example, grandiose assurances about the product's robustness and commercial promise, and/or an eye-catching and high-profile set of non-executive directors (particularly where those directors are not themselves subject-matter experts).

Perhaps the best overarching question that one can ask in respect of a potential investment target is "would I honestly be willing to entrust my own most sensitive and valuable secrets to this company?". The checklist below is designed as a starting-point to assist with answering that fundamental question.

Acknowledgment

The authors should like to thank Robert Allen, a partner at Simmons & Simmons LLP, for his support with and input into this article, particularly on the parts requiring data protection expertise.

Risk assessment	How strong is the business's network(s) and IT security?
	What consideration has been given to cybersecurity during product development?
	Has product testing been carried out, including in appropriate "live" operational environments?
	Does the product/business rely on any third-party performance?
Contract	How does the business routinely contract around, and out of, its commercial risks?
	How are cybersecurity risks limited or apportioned in the contract?
	What is carved out of liability?
	What representations as to security have been given?
	Does the contract counterparty have the financial substance to stand behind its contractual commitments (and to satisfy any damages award against it), and how difficult would it be to enforce those contractual commitments against it?
Business culture	What are the business's security practices like?
	How are passwords distributed within the business?
	What information control policies are in place, and how are these implemented, enforced and periodically reviewed?
	Are employees aware of their personal security responsibilities?
	What auditing is performed in relation to use of/access to/restrictions on/tracking of cloud and other external storage systems?
	Is there regular training on regulatory requirements and security awareness?
Incident response	What incident management and crisis recovery/business continuity policies are in place?
	Is there an incident response team?
	Can the business co-operate with regulators' requests for information and/or access to data?
	Is there appropriate insurance in place to deal with a cybersecurity threat?

Endnotes

1. Around one quarter of the city-state's population.
2. Financial Times, "*Singapore prime minister among 1.5m patients affected by data hack*" (July 2018), available at https://www.ft.com/content/104aa8ec-8c03-11e8-b18d-0181731a0340.
3. In 2017, Cybersecurity Ventures predicated that global healthcare cybersecurity spending would exceed $65 billion cumulatively from 2017–2021 and that ransomware attacks on healthcare organisations would quadruple by 2020 (see Cybersecurity Ventures, "*Healthcare Security $65 Billion Market*" (April 2017), available at https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/).
4. British Standards Institute, "*Cybersecurity of medical devices: Addressing patient safety and the security of patient health information*" (2017), authored by Richard Piggin, Security Consultant (Atkins), available at https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper___Cybersecurity_of_medical_devices.pdf.
5. Wired, "*Medical Devices are the Next Security Nightmare*" (March 2017), available at https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.
6. Reuters, "*J&J warns diabetic patients: Insulin pump vulnerable to hacking*" (October 2016), available at https://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUKKCN12411L.
7. ZDNet, "*FDA issues recall of 465,000 St. Judge pacemakers to patch security holes*" (August 2017), available at https://www.zdnet.com/article/fda-forces-st-jude-pacemaker-recall-to-patch-security-vulnerabilities/.
8. CNN, "*Cheney's defibrillator was modified to prevent hacking*" (October 2013), available at https://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html.
9. Available at https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm.
10. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices.
11. Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices.
12. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices.
13. The MDR will be fully applicable on 26 May 2020. During the transition period, devices can be placed on the market under the current EU Directives, or the new Regulation (if the devices comply fully with the new Regulation) (https://www.gov.uk/guidance/medical-devices-eu-regulations-for-mdr-and-ivdr).
14. MDR, Article 2(1).
15. MDR, Article 2(2).
16. MDR, Annex XVI.
17. MDR, Article 1(5).
18. MDR, Annex I, 14.2.
19. MDR, Annex I, 18.8.
20. MDR, Annex I, 17.4.
21. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
22. The Data Protection Act 1998 has now been repealed and replaced.
23. GDPR, Articles 5(1) and (2).
24. GDPR, Article 4(1). The GDPR defines "data concerning health" as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status" (GDPR, Article 4(15)).

25. GDPR, Article 5(1)(f).
26. GDPR, Article 32(1).
27. Defined as "*…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*" (GDPR, Article 4(5)).
28. GDPR, Article 32(1).
29. GDPR, Article 33.
30. GDPR, Article 33.
31. GDPR, Article 34.
32. For some breaches (including failing to comply with the conditions for processing) data controllers can receive a fine of up to the greater of 4% of global annual turnover for the preceding year (for undertakings) or €20,000,000 (Article 83(5)). For a failure to comply with security obligations, the fine can be up to the greater of 2% of global annual turnover for the preceding year (for undertakings) or €10,000,000 (GDPR, Article 83(4)).
33. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
34. The security and notification requirements do not apply to RDSPs that employ fewer than 50 people, and whose annual turnover and/or balance sheet is less than €10,000,000 (NIS Directive, Article 16(11)).
35. The definition includes: (i) any electronic communications network (as defined under certain EU legislation); (ii) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (iii) digital data stored, processed, retrieved or transmitted by elements covered under (i) or (ii) for the purpose of their operation, use, protection and maintenance (NIS Directive, Article 4(1)).
36. NIS Regulations, Article 11(1).
37. NIS Regulations, Article 12(3).
38. There is no single competent authority; Schedule 1 to the NIS Regulations contains a list of designated competent authorities for particular sectors and sub-sectors.
39. NIS Regulations, Articles 11(3)(b)(i) and 12(6)(a).
40. NIS Regulations, Article 16.
41. NIS Regulations, Article 18(6)(d). This is for a material contravention that the enforcement authority determines has caused, or could cause, an incident resulting in an immediate threat to life or significant adverse impact on the United Kingdom economy. It is understood that a "double jeopardy" scenario will not apply to an incident that breaches both the NIS Regulations and the GDPR, and that a company will only be fined under one of the Regulations, unless the penalties relate to different aspects of the wrongdoing and different impacts (see the government's response to public consultation, "*Security of Network and Information Systems*" (January 2018), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf).
42. In the UK, this implemented Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
43. ICO, "*Private health firm fined £200,000 after IVF patients' confidential conversations revealed online*" (February 2017), available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/02/private-health-firm-fined-200-000-after-ivf-patients-confidential-conversations-revealed-online/.
44. RSM UK, "*Information Commissioner sets out expectations for GDPR enforcement post 25 May 2018*" (25 May 2018), available at https://www.rsmuk.com/ideas-and-insights/information-commissioner-sets-out-expectations-for-gdpr-enforcement-post-25-may-2018.
45. Digiday UK, "*'It's a warning shot': Experts say ICO's fine to Facebook signals seriousness of its GDPR enforcement*" (16 July 2018), available at https://digiday.com/media/warning-shot-experts-say-icos-fine-facebook-signals-seriousness-gdpr-enforcement/.
46. ICO, "*Regulatory Action Policy*" (May 2018), available at https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
47. GDPR, Article 80.
48. [2015] EWCA Civ 311.
49. GDPR, Article 82.
50. Companies Act 2006, s172.
51. Companies Act 2006, s174.
52. See, for example, NCSC, "*10 Steps to Cyber Security*" (August 2016), available at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.
53. Piggin, *Cybersecurity of medical devices*.

Paolo Caldato
Simmons & Simmons LLP
CityPoint
One Ropemaker Street
London EC2Y 9SS
United Kingdom

Tel: +44 20 7825 4621
Email: paolo.caldato@simmons-simmons.com
URL: www.simmons-simmons.com

Paolo is a Managing Associate in the Commercial Litigation group in Simmons & Simmons LLP's London office. His primary focus is on high-tech disputes in the Healthcare & Life Sciences and TMT sectors. Much of Paolo's work involves cross-border litigation for international clients. Paolo's first degree was in the biological sciences (with honours in biochemistry). He is a member of the firm's International Digital Health team, and the Society for Computers and Law. He is also a Tech London Advocate (in the TLA's Health Tech working group), and sits on the Legal Issues and Compliance Committee of the Association of British HealthTech Industries.

David Fitzpatrick
Simmons & Simmons LLP
CityPoint
One Ropemaker Street
London EC2Y 9SS
United Kingdom

Tel: +44 20 7825 5784
Email: david.fitzpatrick@simmons-simmons.com
URL: www.simmons-simmons.com

David is an Associate in the Commercial Litigation group in Simmons & Simmons LLP's Bristol and London offices. He acts for clients on a range of corporate and commercial disputes, often with an international focus and in the Healthcare & Life Sciences and TMT sectors. He has been published on a number of platforms. Prior to joining the firm, David trained at another international law firm in Scotland and spent a year studying in Paris.

Simmons & Simmons

Simmons & Simmons is a leading international law firm with fully integrated teams working through offices in Europe, the Middle East and Asia, bringing experienced professionals to some of the most active growth markets today. We believe it is who we are and how we approach our work that sets us apart from other firms. We set the highest standards for the work we do, meaning you will benefit from the highest quality client service. Our focus on a small number of sectors means we are able to understand and respond to our clients' needs. Our industry sectors are: Asset Management & Investment Funds; Financial Institutions; Life Sciences; and Telecoms, Media & Technology (TMT). We also focus on the E&I market, in particular through our international projects and construction teams. We have a track record for innovation and delivering value to clients through new ways of working.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com