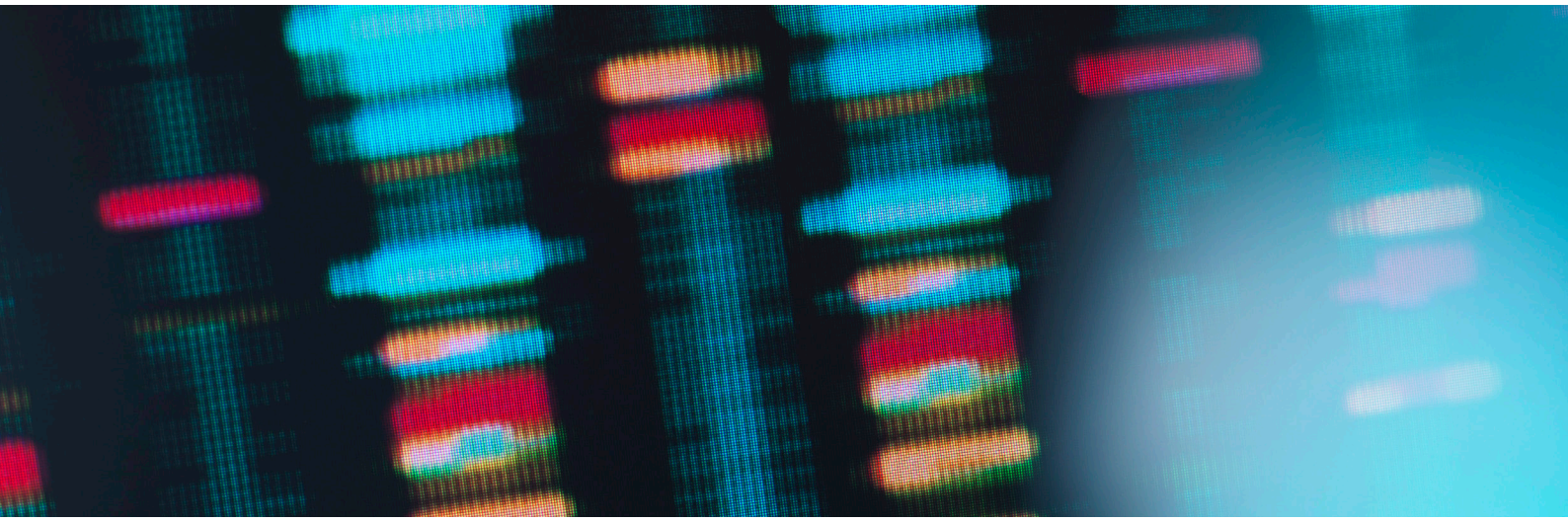
HERBERT SMITH FREEHILLS



Personalised health and cyber security

Personalised health offers great hope for ground-breaking treatments of serious diseases and for early diagnosis and intervention. The ability to sequence a patient's genes at low cost and then use artificial intelligence (AI) to interrogate this data with other phenotypical data will facilitate individualised care and revolutionise healthcare.

With this great promise of data-driven healthcare comes a real risk of cyber-attacks and significant data breaches. The ever-increasing frequency and sophistication of such attacks and the impact of breaches means that great care is needed to ensure that robust security protections are in place over the systems used for the collection and processing of the required data. Recently, the US Food and Drug Administration (**US FDA**) has reiterated the importance of cyber security for medical devices and has increased its activity in the area. The health industry is a key target for cyber criminals, as evidenced by Merck's reported $310 million loss following a cyber-attack in June 2017.

Maintaining patient trust and mitigating technical and legal risks will require a significant investment to ensure robust and compliant systems and processes.

In this article we discuss the exacting and differing requirements of cyber security laws across the world, particularly those in the European Union (EU) General Data Protection Regulation (GDPR), which need to be complied with by those holding and processing data.

Vast quantities of data widely shared

A personal health approach will, out of necessity, involve the collection of vast amounts of highly sensitive personal data. Given the desire to leverage existing patient health information to train and develop beneficial AI, the optimal approach would allow the wide sharing of relevant patient data. Furthermore, as companies develop new tools, such as AI driven diagnostic techniques, the need to share data also increases.
For example, hospitals may be required to provide access to a patient's data (eg, genetic information, test results or scans) to third parties so that they can interrogate those results using relevant algorithms on their servers. However, the more end systems and users that can access data, the more potential end points there will be for malicious actors to access the end user's system.

For example, third parties used by a hospital for interrogation of the personal data, such as biobanks, laboratories and genetic testing services will each have a significant supply chain to which the sensitive personal data could be exposed. Each vendor in the supply chain and their employees must be appropriately vetted to ensure complete protection of the data: it would only take a single employee at one of the vendors to receive and click on a phishing email, for example, and the sensitive personal data would be at serious risk of being exposed.

There is a further risk that third parties may sell, or allow access to, the sensitive personal data. Life insurers, medical insurers and pension providers are just some examples of companies who may gain financially from viewing this data.

An attractive target

Although the theft of large volumes of patient data will involve large transfers of data, as the systems developed and used by companies or health services to transmit and process that data will need to have significant bandwidth and processing power, this will make it easier for malicious actors to extract the data if they can gain access.

Patient data, including genetic data, will undoubtedly be an attractive target for cyber criminals. Malicious actors can be expected to view genetic information as a rich source of potential blackmail – both against the providers and the end users. Providers' reputations will stand and fall on their ability to protect their end users' privacy. Whilst raw patient data such as genetic data may be difficult for an unsophisticated cyber-criminal to exploit directly, if the data has already been interpreted when intercepted to indicate characteristics of the patients themselves, providers may feel as though they have no choice but to pay a ransom to prevent private, potentially embarrassing information from being disclosed and to maintain the patient trust that is critical for the industry.

If the cyber-criminal is a nation state or state-proxy, for example, there is potential for raw patient data to be misused. For example, a malicious actor may be able to correlate the stolen genetic data with biometric data found in a passport or link people together for intelligence purposes. A nation state is likely to have the necessary skills and resources to interpret the data. If this is the case, a genomic dossier could be created linked with other personal details providing the attacker with a very valuable commodity.

Legal requirements

Cyber security law remains in its infancy internationally. However, legislation has been introduced or is being planned to be introduced in most major jurisdictions imposing security obligations on companies dealing in data, particularly when dealing with personal data.

In a future article we will discuss the problems that can arise in determining whether a provider holds enough identifying information for its data to be classified as 'personal data' and therefore subject to the full array of obligations imposed by the GDPR. For this article we focus on the requirements that arise where a provider holds data about identifiable patients.

EU

The GDPR is the EU's main legislative instrument governing the handling of personal data. It came into force on 25 May 2018, superseding all existing member state data protection law based on the successor data protection directive.[1]

Under the GDPR genetic data and data concerning health are each classified as a 'special category' of personal data and subject to higher levels of protection (under article 9) than are given to other types of personal data (under article 6). Bodies processing personal data are required to take appropriate organisational and technical measures to ensure a level of security protection appropriate to the risk (under article 1(f) and 32) and are required to ensure the availability of and access to personal data (under article 32). The GDPR does not prescribe explicit standards of cyber security; the legislation is deliberately worded to require businesses to keep their cyber security under review as threats evolve, and to have controls in place that are appropriate to the risk. Given the high risk posed to individuals of the release of their personal data, providers will be expected to maintain state-of –the-art security controls.

A failure to adhere to the GDPR's requirements can result in significant fines - EUR20 million or 4% of global turnover, whichever is higher. Individuals are entitled to bring claims for damages suffered (both financial and non-financial) as a result of a breach – some jurisdictions will allow class actions to be brought by groups of affected claimants. Failure to keep the systems online could cause serious knock-on effects for patient health and could constitute a compensable breach. Data breaches are required to be notified to the relevant supervisory authority within 72 hours and to be notified to the affected individuals where there is high risk to their rights and freedoms – a standard very likely to be met where the data breached is identifiable patient data.

The GDPR applies to all organisations processing personal data of individuals based within the European Economic Area (EEA), irrespective of where the processing or storage of data takes place.

The EU has also passed a directive on the security of networks and information systems (NIS Directive) which requires certain essential operators in the health sector to implement cyber security protections to ensure resilience and prevent interruption of essential services.

Other jurisdictions

While few other jurisdictions have as mature data privacy laws as the EU, data privacy is an increasing concern to legislators across the world and cyber security is a key component of most new legislation. Australia has recently introduced a mandatory reporting requirement for data breaches. While US data privacy laws

[1] Directive 95/46/EC.

are made at state level and have differing definitions of personal data and different requirements, most states classify breaches of health information as notifiable. The US FDA has also recently published guidance on cyber security and encourages organisations to report any cyber security issues.

What can providers do?

All systems processing patient data should be designed with security and resilience as a core concern. Technical measures such as strong end point security and encryption will be required along with organisational measures to ensure a security-conscious working culture for all employees. Pseudonymisation of data – storing the directly identifying information separately from the rest of the data – should be considered. Given the risks, cyber security should be a board-level concern for providers.

Organisations dealing with patient data should have plans in place to deal with incidents as they arise covering the potential technical, legal, regulatory and publicity repercussions should the worst happen. Supply chains should be sufficiently vetted and appropriate contractual measures must be put in place to enforce minimum standards of security. Organisations should conduct audits on key suppliers to ensure the minimum standards of security are being adhered to. Organisations should also consider whether insurance policies should be taken out to mitigate financially should an attack take place.

Medical devices

Medical devices leveraging personalised health data or using AI such as glucose control mechanisms are already on the market. These devices monitor a patient's blood glucose levels, assesses when to release insulin and send data back to the provider to allow further machine learning. There is potential for all connected devices to be subject to cyber-attack, in the most extreme cases even allowing a perpetrator to take control of the device and, potentially injure or kill the patient for example by changing the dose of insulin.

It is well established that pacemakers that use software or wireless communications are vulnerable to hackers. In 2017, the US FDA and the US Homeland Security issued an urgent alert and recalled approximately 465,000 pacemakers that were vulnerable to hacking. The pacemakers had improper authentication, potentially allowing them to be accessed and sensitive patient information to be transmitted without encryption.

Designers and manufactures need to ensure robust cyber security protections to protect patients and to avoid the potential for product liability law suits.

Conclusion

Personalised health offers great promise but there are real cyber security risks that organisations will need to be conscious of to ensure that the opportunities it presents are not eclipsed by the risks. Patient trust is the key enabler for personalised health. If a cyber-attack takes place, and personal information is exposed, this trust will be lost irretrievably causing irreparable damage to the provider.

Key contacts

Andrew Moir
Partner
T +44 20 7466 2773
andrew.moir@hsf.com

Peter FitzPatrick
Associate (Australia)
T +44 20 7466 3711
peter.fitzpatrick@hsf.com

Jonathan Turnbull
Partner
T +44 20 7466 2174
jonathan.turnbull@hsf.com

HERBERTSMITHFREEHILLS.COM

BANGKOK
Herbert Smith Freehills (Thailand) Ltd

BEIJING
Herbert Smith Freehills LLP
Beijing Representative Office (UK)

BELFAST
Herbert Smith Freehills LLP

BERLIN
Herbert Smith Freehills Germany LLP

BRISBANE
Herbert Smith Freehills

BRUSSELS
Herbert Smith Freehills LLP

DUBAI
Herbert Smith Freehills LLP

DÜSSELDORF
Herbert Smith Freehills Germany LLP

FRANKFURT
Herbert Smith Freehills Germany LLP

HONG KONG
Herbert Smith Freehills

JAKARTA
Hiswara Bunjamin and Tandjung
Herbert Smith Freehills LLP associated firm

JOHANNESBURG
Herbert Smith Freehills South Africa LLP

KUALA LUMPUR
Herbert Smith Freehills LLP
LLP0010119-FGN

LONDON
Herbert Smith Freehills LLP

MADRID
Herbert Smith Freehills Spain LLP

MELBOURNE
Herbert Smith Freehills

MILAN
Studio Legale Associato in association with
Herbert Smith Freehills LLP

MOSCOW
Herbert Smith Freehills CIS LLP

NEW YORK
Herbert Smith Freehills New York LLP

PARIS
Herbert Smith Freehills Paris LLP

PERTH
Herbert Smith Freehills

RIYADH
The Law Office of Mohammed Altammami
Herbert Smith Freehills LLP associated firm

SEOUL
Herbert Smith Freehills LLP
Foreign Legal Consultant Office

SHANGHAI
Herbert Smith Freehills LLP
Shanghai Representative Office (UK)

SINGAPORE
Herbert Smith Freehills LLP

SYDNEY
Herbert Smith Freehills

TOKYO
Herbert Smith Freehills