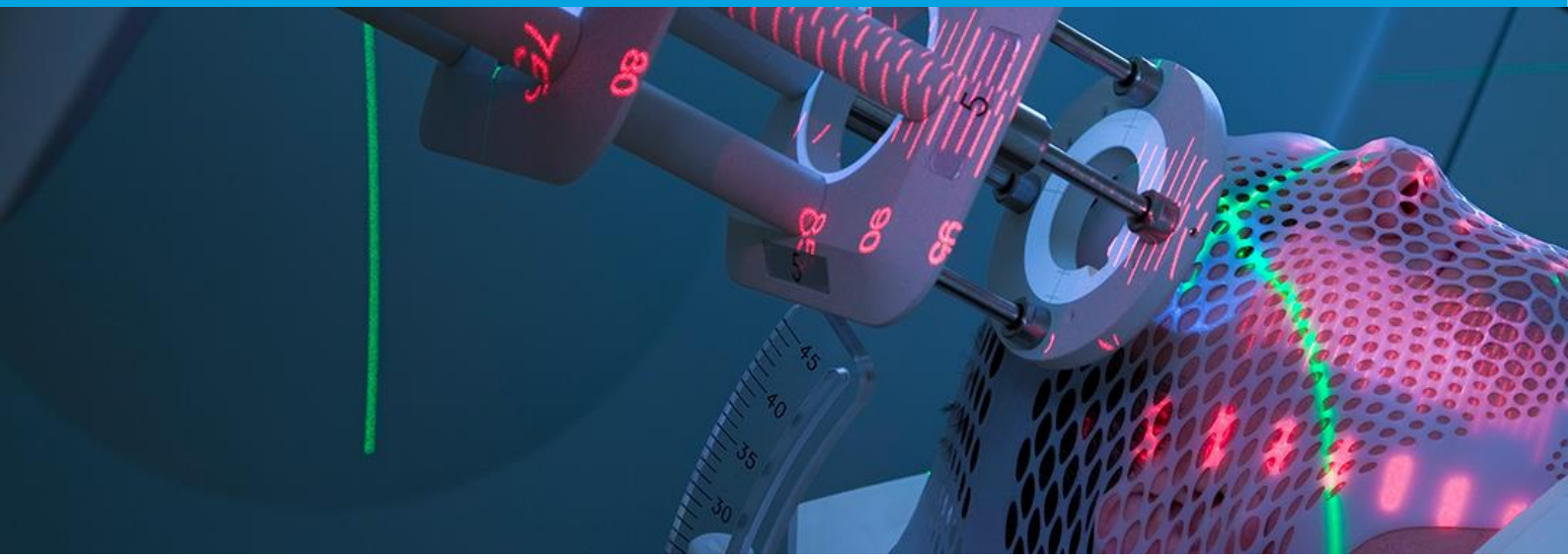
The future of healthtech:
A global perspective

Asia Pacific | Europe | Latin America

March 2022

Kennedys

Contents



Foreword

Technological advancements offer significant opportunities and benefits in the delivery of healthcare, but also present new and significant risks for the healthcare sector.

In May 2021 we launched our Healthtech in the future - the legal ramifications report, with developments in healthtech and emerging risks for the healthcare sector explored through the lens of the current legal and regulatory framework in the United Kingdom.

Now in this global update Kennedys' medical malpractice specialists across the globe consider the extent to which healthtech will challenge the underlying basis of the legal obligations currently owed by clinicians and healthcare providers, as well as exploring cyber and data privacy risks for the healthcare sector globally.

Providing unique insights into the existing legislative and regulatory landscape in their jurisdictions - and the extent to which change will be required — we also identify where healthtech related claims are starting to emerge and offer recommendations to help mitigate against potential risks.

The COVID-19 pandemic has undoubtedly accelerated the adoption of technological developments in healthcare and highlighted its potential wider application. The use of healthtech will inevitably continue to increase, develop and evolve and having the right framework will be essential.

Key contact

Christopher Malla
Global Head of Healthcare, London
t +44 20 7667 9194
e christopher.malla@kennedyslaw.com

Edited by

Roger Davis
Corporate Affairs Lawyer, London
t +44 207 667 9046
e roger.davis@kennedyslaw.com

About Kennedys

Healthcare is one of the most complex, fastest growing and heavily regulated industries, requiring specialised legal representation and a law firm that will help you think ahead. We're a fresh-thinking firm, and not afraid to bring new ideas to the table beyond the traditional realm of legal services.

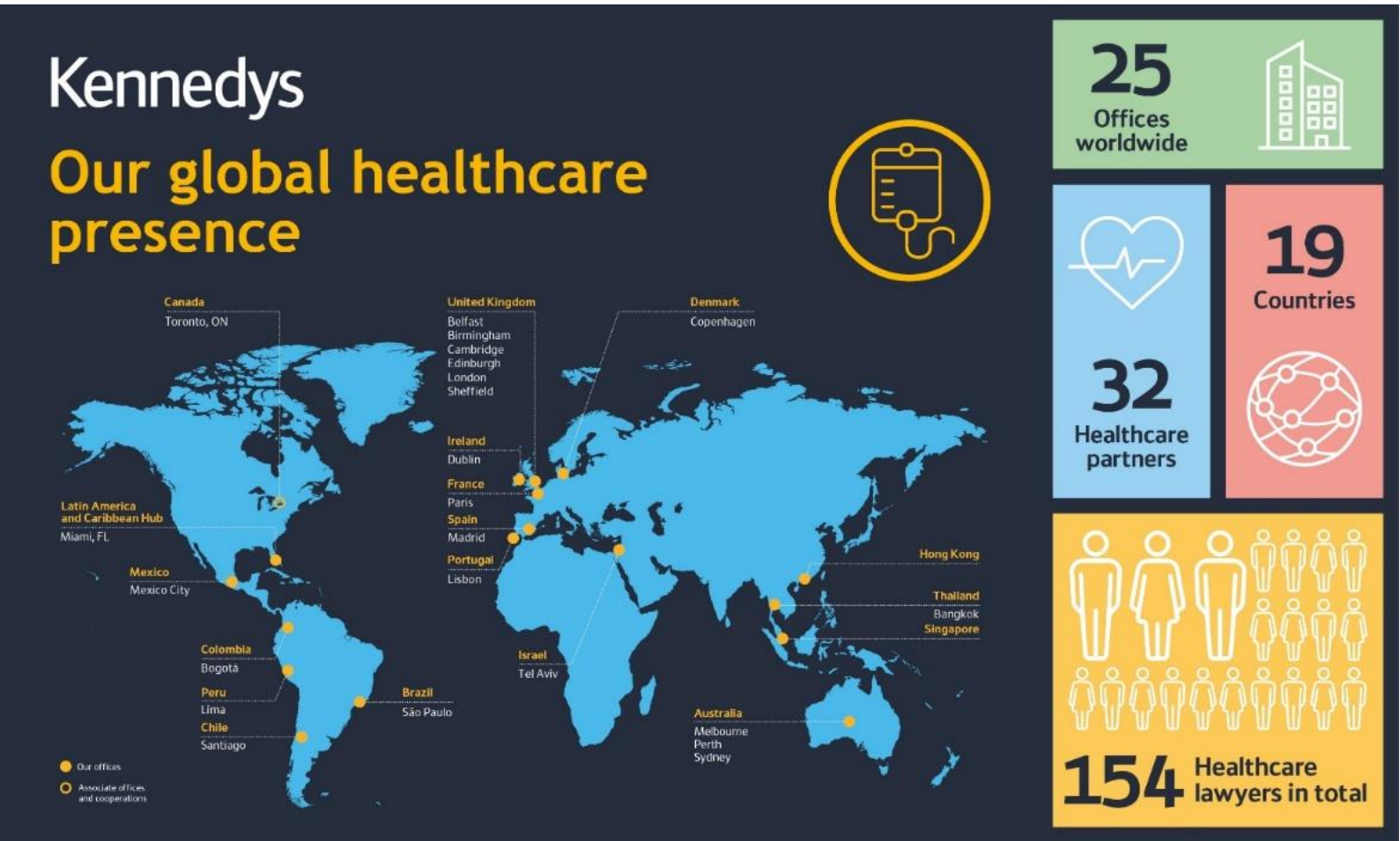
Kennedys is a global law firm with particular expertise in litigation and dispute resolution, especially in defending insurance and liability claims. Our global, market-leading healthcare team has over 30 years' experience in successfully handling medical negligence claims and advising on clinical and health law issues.

Working with both private and public sectors, healthcare professionals and their insurers, Kennedys' legal and clinical experts across the world handle medico-legal matters on an international scale. Our team have significant experience in acting for a range of complex civil and multi-jurisdictional claims, along with managing both contentious and non-contentious matters.

Acting across jurisdictions and in both the public and private healthcare sectors gives us a unique understanding of healthcare law from every perspective. This enables Kennedys to deliver straightforward advice to clients, even when the issues are complex.

Global reach / Local expertise

kennedyslaw.com/healthcare



Asia Pacific

Australia

Whilst the COVID-19 pandemic has resulted in an increase in the uptake of healthtech in Australia, development and utilisation of such technology remains relatively slow.[1]

Artificial intelligence and robotic surgery

Artificial intelligence (AI) technology has been used in clinical settings in Australia:

> **"In clinical settings, AI is being used to provide earlier and more accurate diagnosis of cancer, infectious disease and other forms of illness."[2]**
>
> *Stefan Hajkowicz et al*

Robotic surgery has also become increasingly widespread and has "predominately been adopted by urology, gynaecology and most recently, general surgery in the private sector".[3]

At present, AI in clinical settings and robotic surgery in Australia is not fully automated, with doctors still having control and the ability to override the judgement made by AI.

Once AI takes on more autonomous decision making the question of liability will become more complicated and we anticipate Australia's legal framework[4], including the current Therapeutic Goods Administration (TGA) regulations[5], will need to change to ensure its legal principles are responsive to the new technology.[6]

More generally, as AI healthtech becomes further developed and utilised in Australia, it will challenge the standards of care owed by healthcare professionals and may form part of such standards.

Virtual healthcare

Virtual hospitals, wearable devices to monitor vital signs, telehealth appointments and electronic prescriptions are all now being utilised across the country and there are opportunities to build on the use of remote and virtual care that has taken place during the pandemic.

These developments do, however, present risks and we are beginning to see claims for misdiagnosis or delays in diagnosis as a result of virtual medicine and the inability or failure to arrange a physical examination.

Genomics

As observed in the National Health Genomics Policy Framework:

> **"Genomics has the potential to reshape clinical practice and to fundamentally change the way we prevent, diagnose, treat and monitor illness."[7]**
>
> *National Health Genomics Policy Framework*

However, the use of genomics also raises complex legal and ethical issues for Australian healthcare professionals. In Australia, healthcare professionals cannot breach their duty of confidentiality and disclose genetic information to at risk genetic relatives without the patient's consent.

The only exception is where they reasonably believe that the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of the genetic relative (s.16B(4) of the Privacy Act 1988 (the Act).

However, this legislation only offers protection from statutory liability under the Act and does not purport to affect the common law obligation of confidentiality.[8]

The Act also only applies to Australian government agencies and private institutions and does not apply to state entities such as public hospitals.

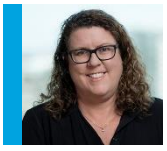
> **As the use of genomics develops further, we anticipate that a more coherent national legal framework will be necessary.**

While in other countries insurers are banned or restricted from using genomic results in underwriting, in Australia (in respect of life insurance policies) there is a moratorium in place until 30 June 2024:

> **"[The moratorium] prevents insurance companies from using genetic test results as part of the risk assessment for insurance policies up to A$500,000 for death or total permanent disability.[9]"**
>
> ***Centre for Genetics Education***

Contacts

Cindy Tucker
Partner, Melbourne
t +61 3 9498 6607
e cindy.tucker@kennedyslaw.com



Raylee Hartwell
Partner, Sydney
t +61 2 8215 5909
e raylee.hartwell@kennedyslaw.com

Anjali Woodford
Partner, Melbourne
t +61 3 9498 6609
e anjali.woodford@kennedyslaw.com

Rosie Blakey-Scholes
Senior Associate, Perth
t +61 8 6147 4380
e rosie.blakey-scholes@kennedyslaw.com

Hong Kong

The use of technology in the healthcare context is a global trend, and Hong Kong is no exception.

Technologies have been integrated in various ways for the provision and receipt of care, including a surge in telemedicine mobile applications and teledentistry companies in the city.

Telemedicine mobile apps

The COVID-19 pandemic has accelerated the adoption of telemedicine in view of the higher risk of infection associated with consultations at hospitals or clinics, and the shortage of medical resources.

> **Major private hospitals, leading insurance companies, and large telecommunication companies have individually or jointly rolled out different mobile applications to provide teleconsultations and deliver treatments.**

Undeniably, telemedicine allows patients, especially those who are elderly and/or with disabilities, to receive medical care with less time, effort and risks. It equally helps healthcare professionals to remotely and conveniently monitor a patient's condition through online consultations and constant updates of health data.[10]

Telemedicine, nevertheless, is not risk-free. As highlighted in the Ethical Guidelines on Practice of Telemedicine (the Guidelines) issued by the Medical Council of Hong Kong (the Medical Council), the fact that telemedicine precludes physical examinations increases the inherent risks in providing treatments.

In accordance with the Code of Professional Conduct issued by the Medical Council, the responsibility for dispensing medications is borne by doctors. The process of prescribing by the doctor remains the same, whether delivered by courier or dispensed face-to-face.

Substitution of face-to-face consultations also means medical practitioners have to rely on courier services to dispense medications. The doctor will remain responsible for the medications dispensed in the event of any errors/problems arising during the courier's delivery to the patient.

> **Whilst we are not currently aware of any claims in relation to errors arising from this remote means of dispensing medication, liability is unclear should deliveries go wrong.**

With telemedicine continuing to be a fast-growing method of healthcare delivery it is questionable whether medical practitioners will be able to adhere to the Guidelines and only practice telemedicine with patients where they have a prior in-person doctor/patient relationship.

These examples reflect how telemedicine will complicate the doctor/patient relationship by adding intermediaries in between. This challenges the basis of legal obligations owed by healthcare professionals, raising the question as to whether these intermediaries share the legal responsibilities of healthcare professionals, and if so, how?

Orthodontic treatments through teledentistry

Aesthetic orthodontic treatments can now be provided through a combination of online consultations and utilisation of 3D technologies with minimal assistance. This treatment method has presented itself as a convenient alternative to the traditional, time-consuming, and costly teeth aligning procedures.

The benefits may sound attractive to many, however orthodontic treatments effected wholly through online consultations and technologies controlled by patients is concerning as it may

leave consumers without protection in the event that injury or damage occurs.

Without direct assistance from dentists throughout the process of teeth aligning, service providers may avoid liabilities by being outside of the definition of 'practicing dentistry' under the Dentists Registration Ordinance. Even with online consultations provided by overseas-qualified dentists, their services would not be regulated by the Dental Council of Hong Kong (the Dental Council).

In light of the prevalence of this type of teledentistry, the Dental Council and the Hong Kong Society of Orthodontists issued a joint statement in December 2019 warning the public that orthodontic treatments are professional dental treatments which should be carried out and supervised by registered dentists.

Implications

As healthtech advancements continue to develop, professional bodies including the Medical Council and the Dental Council will need to update the professional codes of conduct to provide clearer guidance to healthcare professionals.

Amendments to existing legislation or the enactment of new legislation to close potential loopholes and to protect the general public from unregulated healthcare services may be required.

Whilst time is needed for the legal and regulatory framework to catch up, healthcare professionals should remain vigilant in providing treatments through virtual platforms.

The overarching principle must be kept in mind that when providing healthcare/treatment through virtual/remote platforms medical professionals are subject to the same standard of care, as that which is applicable in face-to-face scenarios.

Contacts

Christine Tsang
Partner, Hong Kong
t +852 2848 6350
e christine.tsang@kennedyslaw.com

Sandy Cho
Partner, Hong Kong
t +852 2848 6344
e sandy.cho@kennedyslaw.com

Ricky Wu
Senior Associate, Hong Kong
t +852 2848 6304
e ricky.wu@kennedyslaw.com

Thailand

Due to the COVID-19 pandemic, telemedicine in the form of online/virtual clinics have become an important pathway enabling patients to consult with their doctors remotely. The use of telemedicine had been authorised prior to the pandemic by the Medical Council of Thailand under notification No. 54/2563.

Medical services must still comply with the medical standard applicable to non-remote delivery of healthcare. In the absence of clear guidelines or a regulatory framework, the importance the Supreme Court of Thailand has placed on a physical examination must be kept in mind — observing that it is an essential procedure in the diagnosis of a patient's symptoms, the state of disease or pathology, leading to appropriate treatment.

The main challenge for healthcare providers is that medical malpractice claims are governed by the Consumer Case Procedure Act, which places the burden on healthcare providers to prove that they have not been negligent.

As the use of healthtech within the healthcare sector in Thailand increases, we anticipate it will be necessary for changes to be made to the current legal and regulatory framework.

According to notification No. 54/2563 of the Medical Council of Thailand, only telemedicine or online clinics are permitted. However, there is no legal framework regulating other aspects of the provision of healthtech by healthcare organisations.

Below are examples of where a legislative framework to provide clarity is required:

- As to whether or not healthcare providers would require an additional license to develop and use other types of healthtech (beyond telemedicine) in the delivery of healthcare.
- What safeguards may be required to ensure the privacy and security of patients' personal health information.
- How the medical standard is to be determined if the medical service is rendered through healthtech or with the assistance of healthtech, particularly, to what extent healthtech can be applied by healthcare providers.

Furthermore, under Thai law it is currently unclear whether healthtech is considered medical equipment or normal manufactured goods and where liability would rest in the event of any injury or loss sustained by the patient. For example, whether liability would rest with the healthcare provider (who applies the healthtech) or the developer of such healthtech (if not developed by the healthcare provider).

We are not currently aware of any medical malpractice claims arising from the use of healthtech. However, a Thai court has ruled that giving a diagnosis via telephone without physical examination, which led to misdiagnosis of the patient's condition, may be considered medical malpractice.

We would therefore anticipate that claims relating to remote/virtual forms of healthcare may arise in the near future.

Recommendations

To help safeguard both patients and healthcare professionals against the potential risks that these technological developments present, a conversation or consultation between healthcare professionals and patients should be recorded.

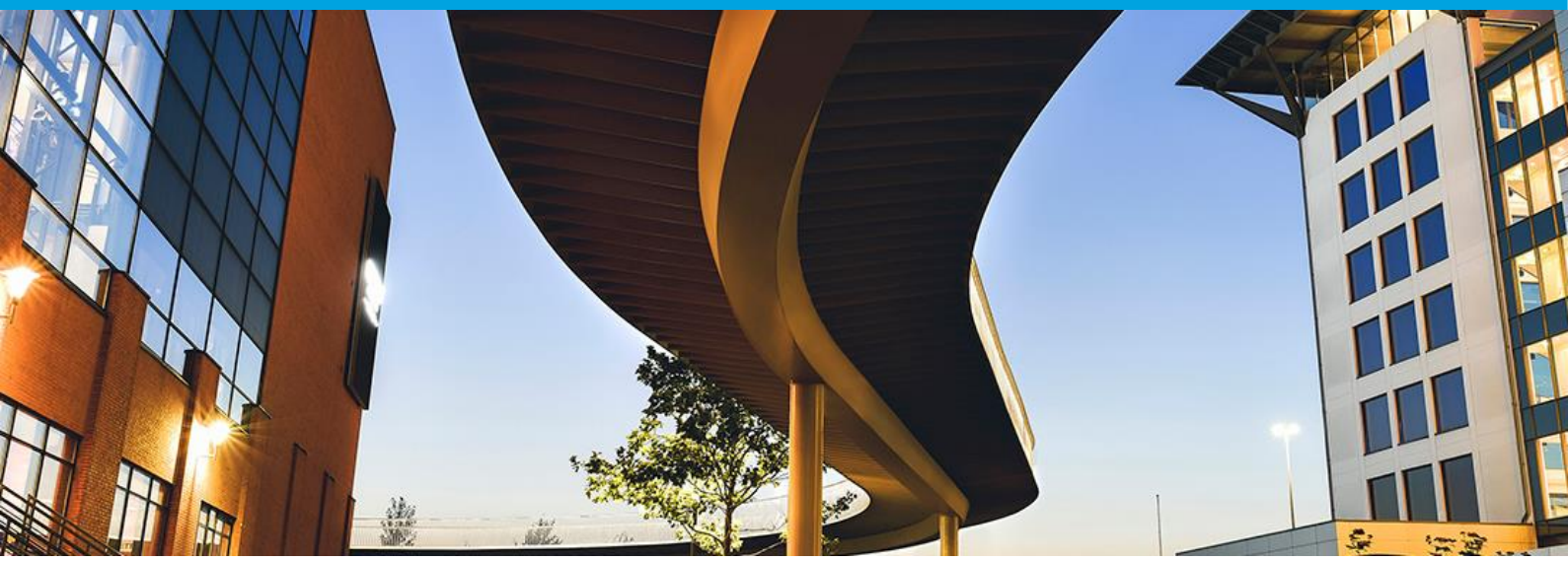
Such record would form part of the patient's medical records. In Thailand, the court often relies on medical records when determining if there is medical malpractice, with consideration given to what has or has not been recorded. Prior to such conversations or consultations being recorded, informed consent must be obtained from the patients in advance.

Healthcare providers must also ensure that all information held electronically through a form of healthtech is kept securely and strictly confidential, and in compliance with the law governing personal data protection.

Contact

Tassanu Chutikanon
Special Counsel, Bangkok
t +66 2 491 4803
e tassanu.chutikanon@kennedyslaw.com

Europe



Denmark

Currently, healthcare providers in Denmark have a legal obligation to provide compensation for patients that have been injured whilst being examined or treated.

This obligation arises through LBKG 2018-06-14 nr 995 Klage — og erstatningsadgang inden for sundhedsvæsenet (§§ 19-23), which are regulations that cover a wide ambit of claims arising from medical treatment. Specifically § 19, provides compensation in general for injury/harm which a patient has sustained while being examined or treated at a hospital or by employees of that hospital.

The damages are paid by Patienterstatningen, the Danish authority that covers compensation payable for claims within the healthcare sector.

With that in mind, we do not anticipate that in Denmark advancements in technology utilised to treat and care for patients will necessarily change the overarching legal obligations owed by healthcare providers.

The current regulations governing compensation for patients are wide in terms of the circumstances covered. However, there may be borderline cases where the use of technological advancements, may/would not be covered by the current legal framework.

For example, where patients are treated remotely through robotic surgery. In circumstances where the surgeon is controlling the robot performing the surgery, we anticipate that a claim arising would still be covered by §19.

However, questions arise as to how and/or whether the regulations would still apply in circumstances where injury/harm arises should the injury/harm arise at a point where the surgeon is not controlling the robot.

Whilst this particular technology is not currently utilised in Denmark, we anticipate that the current regulations will need to be adapted to provide clarity in relation to claims arising from technological advancements in the delivery of healthcare, such as robotic surgery.

Emerging claims

Claims arising from healthtech are beginning to emerge in Denmark.

One example of this is in the context of wearables and patient self-management, where claims relating to faulty respiration and sleep-apnea devices have been brought (where the minimum loss that claimant is seeking to recover is DKK 8209 (the equivalent of approximately £921)). Patienterstatningen has provided compensation for damages in connection with the use of devices of this type.

Contact

Thomas Arleth
Senior Associate (Advokat, H), Copenhagen
t +45 33 73 70 53
e thomas.arleth@kennedyslaw.com

England

Modern healthcare is built on the premise that treatment is a shared decision between a doctor and a patient, with the role of technology now increasingly a part of that conversation, with a definite shift towards greater patient autonomy through new virtual healthcare initiatives.

Whilst the UK's current legal and regulatory framework provides a foundation for future healthtech developments, it will undoubtedly need to be modified as technological innovation and its application in healthcare continues to evolve.

A new focus on legal liability is required, for example regarding:

- Increasing implementation of genetic profiling for precision medicine.
- The delivery of care remotely in both the primary and secondary care setting.
- The use of artificial intelligence both in primary care and clinical elements of healthcare.
- Wearable technology.
- Robotic assisted surgery.

> **For the foreseeable future at least, clinicians are still likely to be making clinical judgements as to patient care and treatment alongside healthtech.**

What duty of care will attach to clinicians who utilise healthtech in treating patients is likely to be an issue to be determined by the courts in due course, and we envisage the laws on non-delegable duties of care becoming more sophisticated.

Causation

The complex chain of causation in healthtech means that the identification of the cause of any harm to a patient is likely to become more challenging.

We may therefore also see development in the law on causation to facilitate patient redress in circumstances where there are a number of potential defendants, to include healthcare providers such as the NHS and private healthcare providers, and where the exact cause of harm cannot be identified.

> **At present both existing legal frameworks (i.e. the tortious route and the statutory and contractual route) could apply in unison; to be adapted as the courts see fit.**

As future case law is set, we may see some blurring of these two areas of law to create hybrid legal principles, including new duties of care on clinicians to ensure that patients have a right of redress should they suffer harm as a result of healthtech in operation.

Similarly, a non-delegable duty of care may arise for healthtech manufacturers and software developers, knowing their products and devices will be used on and by patients.

Duty of care

Whilst the current legal framework provides a good basis for liability risk presented by healthtech in a clinical setting, changes are likely to be required over time.

This is to account in particular for harm caused by AI to patients such as missed diagnosis or inaccurate triage and the impact it is likely to have on clinicians' duty of care in the treatment of patients and their responsibility for AI operated treatment systems.

A clinician's greater involvement/duty of care in the supply of medical devices to patients along with advice they provide to patients as to their use and operation, will also need to be factored in to that legal framework.

We anticipate much of the discussion on duty of care will come down to the control which any potential defendant reasonably had over the product or device.

Such control might reasonably be found to rest more with the manufacturer, software developer and/or maintenance contractor, than the clinician or healthcare providers as a whole.

Regulators

We also anticipate that the role of UK healthcare regulators will need to change, as the use of healthtech within the healthcare sector develops.

The Care Quality Commission, NHS Digital, and the Medical and Healthcare Products Regulatory Agency are likely to have a major and collaborative role to play, alongside the newly created NHSX.

Recommendations

Future proofing to mitigate against the risks that these technological developments bring will require a multifaceted approach, including:

- The need for increased training for healthcare provider staff to ensure that risks to patients are anticipated and minimised.
- A robust approach to limitation of liability through the negotiation of contracts and license agreements with developers/producers/manufacturers/other third parties, to ensure appropriate indemnities are in place.
- Investment in IT infrastructure and cyber protection to minimise risk of data breaches and unauthorised data capture.
- Increased investment in healthcare provider's hardware and infrastructure at every level.
- Appropriate regulation and accreditation will be required for the safe use of new apps, artificial intelligence, wearables and robotics in the treatment of patients.

It is hoped that the UK Government will take steps through appropriate regulation to help protect healthcare providers from significant exposure to risk and compensation payments due to healthtech.

However, balance will need to be found to ensure that patients have protection and clear rights of redress where harm arises from a situation in which healthtech has been utilised to treat a patient.

Healthcare professionals have, for years, adopted and adapted to using new technology. Holding consultations with patients and inputting clinical information in real-time is not new. What has changed is public willingness to engage with such technology, by necessity.

Growth in online consultations is one of the most noticeable developments during the pandemic, and the profile of digital health technology has been raised as a result.

The large-scale adoption of technology is yet to be fully evaluated, however this level of acceleration in use of digital healthcare technology brings with it continued consideration of patient safety. What may aid the argument that quality has been improved via digital healthcare is evidencing by way of standards being met.

Testing, and independent assessment, by the health and social care system building public confidence in such systems.

Related items

- Healthtech in the future – the legal ramifications
- Digital healthcare and patient safety – the journey continues
- Healthcare: the operational and digital response to COVID-19
- Digital solutions in healthcare as we emerge from the pandemic

Contacts

Rob Tobin
Partner, Cambridge
t +44 1223 533 095
e rob.tobin@kennedyslaw.com

Camilla Long
Partner, Cambridge
t +44 1223 533 182
e camilla.long@kennedyslaw.com

Ed Glasgow
Partner, London
t +44 20 7667 9129
e ed.glasgow@kennedyslaw.com

France

According to France Biotech, more than 400 companies have emerged in the medical sector over the last year. This includes Biotechs (49%), Medtechs (18%) as well as companies in the E-health sector (12%)[11].

This transformation of the medical sector, which has undoubtedly been accelerated during the COVID-19 pandemic, challenges the obligations owed by healthcare providers.

Confidentiality: patient data

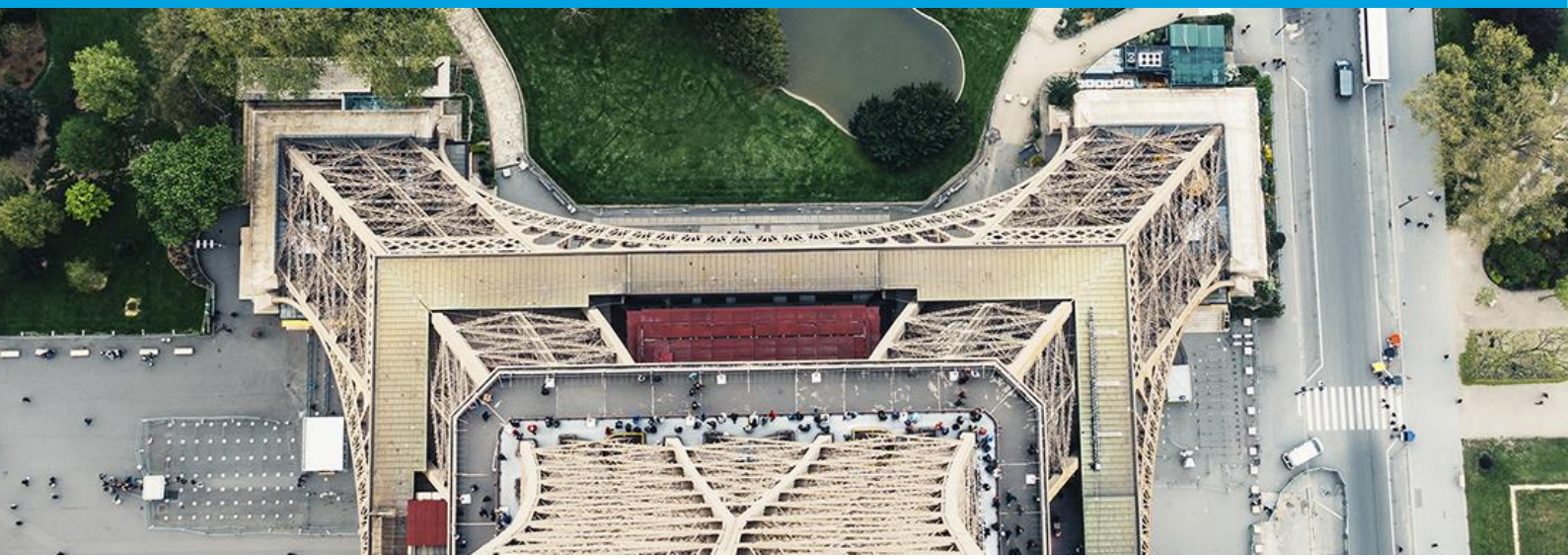
Strict ethical duties, including medical confidentiality, to which French doctors are subject, are particularly likely to be at risk from the development of new technologies.

For instance, several medical devices, or platforms providing teleconsultations, require disclosure of the patient's personal data, meaning access is no longer restricted to medical practitioners only.

The increase in the number of third parties between a patient and the doctor, particularly in the context of telemedicine, presents a number of risks, particularly in relation to the protection of confidential patient data, and is likely to bring substantial legal issues.

In the context of tele-expertise, a doctor is able to exchange medical advice with other health providers. Moreover, tele-assistance technology enables medical practitioners to request the intervention of a colleague when performing certain medical procedures.

These technological advancements raise questions on the nature and the extent of the liability that might be incurred in case of injury and provide examples of the type of issues that will need to be addressed through changes to France's existing legal and regulatory framework.



Emerging claims

Several claims in relation to new technologies in the medical sector have been filed before French Courts, particularly during the last few months, demonstrating the need to adapt the current legal framework.

For instance, medical practitioners have recently challenged the validity of the partnership between the French platform Doctolib and the Ministry of Health to allow people to book their COVID-19 vaccine appointment.

However, on 12 March 2021, the Conseil d'Etat - the highest French administrative court - rejected their claim, holding that the platform met all the required conditions in terms of data storage.

We anticipate that this claim will be followed by others in the context of the COVID-19 pandemic.

Indeed, the new restrictions adopted by the government, such as the obligation to present a 'health pass' to be authorised to exercise certain activities (and notably to enter a large number of public places) is likely to lead to new claims.

Individuals and associations have already filed requests before the Conseil d'Etat's urgent application judge to try and obtain the suspension of this obligation in some places, arguing notably that the 'health pass', in its digital version, does not protect privacy rights and data protection rights.

The French National Authority for Health regularly publishes guidelines and recommendations, including those on new technologies designed to treat and care for patients. For instance, a guide on teleconsultations and tele-expertise has been accessible online since May 2019.

We recommend healthcare organisations, medical professionals and patients access these guidelines to support their understanding of the extent of any rights and/or obligations applicable to them.

Despite teleconsultations presenting difficulties in making a diagnosis in some circumstances — where an in-person examination may assist - there is no distinct medical liability regime in place for this means of delivering healthcare.

Prior to the pandemic 'e-health' (healthcare services provided electronically) was already a rapidly expanding market, bringing with it the emergence of new risks in relation to professional liability of medical practitioners and healthcare institutions.

Contact

Aurélia Cadain
Partner, Paris
t +33 1 84 79 37 82
e aurelia.cadain@kennedyslaw.com

Portugal

A significant challenge when implementing new technological innovation in the delivery of healthcare is understanding where liability rests — if things go wrong — in respect of the supplier, the healthcare provider (clinic or hospital) or the doctor that uses the technology.

Case law

In recent years, Portuguese case law has applied either civil liability or tort liability in cases concerning the responsibility of healthcare providers and medical acts.

In most circumstances, it is possible either to apply civil liability or tort/extra-contractual civil liability. However, as a rule, contractual liability is more favourable to the injured party, and because of that, patients usually choose to apply this one when pursuing a claim.

> **In the context of AI and, therefore, where there are potentially multiple causes of the damage sustained, it is essential to consider whether the damage could have been avoided, by action or omission.**

In doing so, it is necessary to take into account the principle of *bonus pater familias* (i.e. the standard of care and diligence expected of an individual in certain circumstances) by the person who was using the technology. Or, if on the contrary, the damage was caused as a result of incorrectly supplied data or defects in the technology. If it is the latter, Portuguese courts are likely to apply product liability rules.

> **The use of robots and machines in diagnosis and patient treatment will have repercussions on the current legal system in Portugal.**

We may move from civil liability or tort/extra-contractual liability to product liability, or perhaps to a new institute (i.e. a new legal obligation). Portugal has not yet approved any specific legislation regarding this matter.

We believe legislation should be adjusted in accordance with the evolution and technological development, covering issues including:

- Civil liability
- Compulsory insurance
- Product liability
- Criminal liability
- Personal data protection.

Potential claims

The impact of the implementation of healthtech on the claims landscape in Portugal is as yet unknown. With regard to remote consultations, we anticipate an increased risk of medical malpractice claims related to misdiagnosis and late diagnosis.

We believe that it is necessary to define the acceptable level of risk and manage risk reduction.

Double checking systems (i.e. where the result identified by the artificial intelligence is then checked by the doctor), and drawing up codes of conduct and clear rules of procedure for healthcare professionals are steps that should help to mitigate against potential risks.

We agree with those who argue that the principles for dealing with risk are "anticipation, prevention, detection and reaction".

Contacts

Paulo Almeida
Partner, Lisbon
t +351 21 324 36 90
e paulo.almeida@kennedyslaw.com

Marta Oliveira
Senior Associate, Lisbon
t +351 21 324 3690
e marta.oliveira@kennedyslaw.com

Spain

In the past decade, Spanish case law has made clear that the general obligation of medical professionals is one of means rather than a result. In other words, treatments must be in accordance with professional protocols but recognising that achieving an end result is beyond the control of medical professionals - irrespective of whether the treatment is curative or voluntary.

This is the case unless there is a clear contractual stipulation for an end result (which for example, would be more likely in relation to cosmetic procedures).

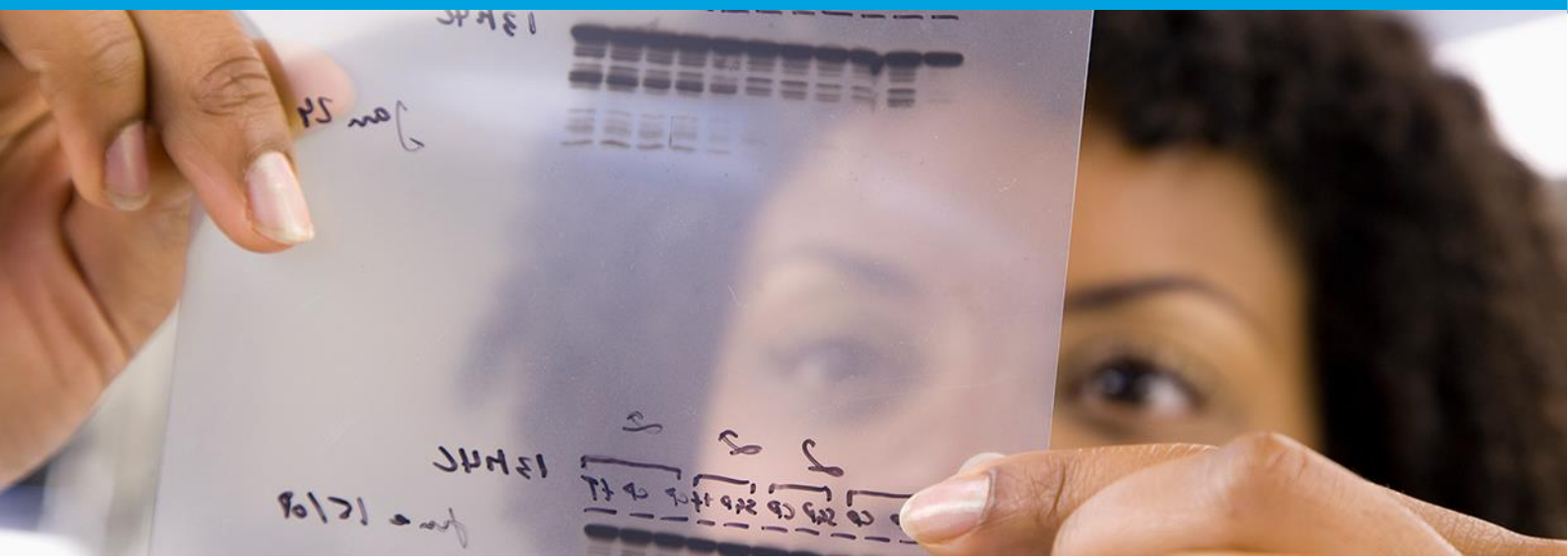
We anticipate that this doctrine will be maintained when applied to the application of technological advances where human input remains crucial.

For example, even if a surgical procedure is robotically assisted, we would not foresee an obligation of results will supersede the current criteria of an obligation of means.

Liability

Nevertheless, partly as result of changing social attitudes, civil liability in environmental law in relation to both legislation and case law has shifted towards strict liability.

It is conceivable that results-based liability or even strict liability could be applied to medical



procedures where losses are a result of failings in the technology rather than due to human error.

Social pressure may result in calls for the healthcare sector to be held to higher standards if it is perceived that the technological advances are being imposed on patients, especially if traditional treatments are phased out.

Future framework

We anticipate that the legal and regulatory framework in Spain will require updating as technological advances become more prominent in the healthcare sector.

> **Legislators will need to strike a difficult balance between regulation (safeguarding patients), and ensuring that patient care does not suffer as a result of denying the entry of new technological advances.**

We also anticipate that the role of healthcare regulators will take on increasing importance in authorising the implementation of technological advances and communicating the efficacy of new methods of healthcare delivery.

To date, emerging areas of healthtech are not giving rise to a volume of cases in Spain. Case law has yet to set precedents which could affect the implementation of new methods and approaches in the healthcare sector.

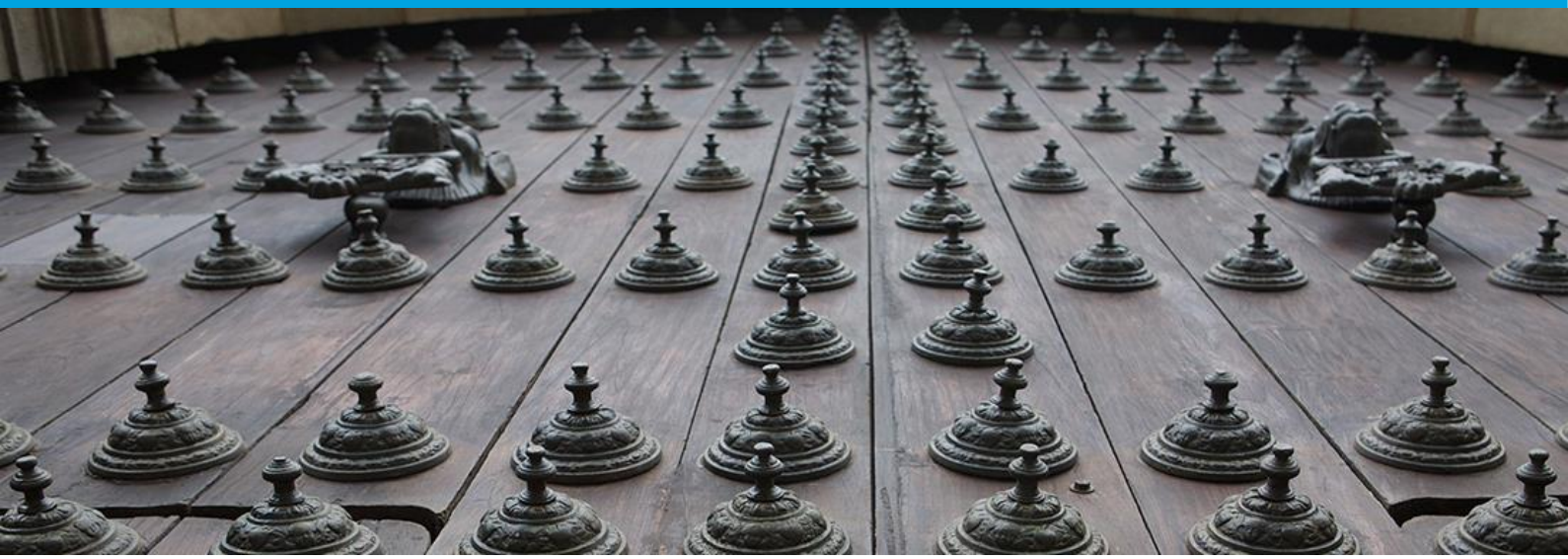
> **We anticipate that informed consent will play an increasingly important role in the implementation of technological advances.**

This will be to ensure that patients are fully aware of new treatments and any risks associated with those, as well as providing full information on the availability of alternative methods of treatment (and the risks and benefits of those).

Contact

Alfonso de Ramos
Partner, Madrid
t +34 919 17 04 02
e alfonso.deramos@kennedyslaw.com

Latin America



Peru

Technological advancements utilised to treat and care for patients will definitely challenge the underlying basis of the legal obligations currently owed by healthcare providers in Peru.

Since 2016, Peru has developed an incipient legislative framework for the use of telemedicine, which is restricted to the use of information and communication technology in the provision of healthcare services, and has provided new legal obligations for healthcare providers, which include:

- Progressively incorporating telemedicine in their services portfolio.
- Having adequate technology equipment and tools needed for the generation of virtual prescriptions.
- Using a communication method and system for storage of information that ensures the confidentiality, integrity and availability of the information.

Legislators will need to strike a difficult balance between regulation (safeguarding patients), and ensuring that patient care does not suffer as a result of denying the entry of new technological advances.

However, inevitably these advancements will bring new responsibilities and legal obligations for healthcare providers, and the current legislative framework will need to be adapted to reflect each technological advancement.

Legal and regulatory framework

The initial use of healthtech has already demonstrated the need for numerous changes in the current Peruvian legal and regulatory framework.

One important change that has been made was the introduction of the Telemedicine General Law, enacted in 2016, which creates the National Commission of Telehealth (Conatel), a new regulatory entity attached to the Ministry of Health. Conatel is responsible for the implementation, supervision and suggestions for improvement to the Telemedicine National Plan.

Challenges

One of the main challenges faced by the healthcare sector in Peru is the absence of an integrated healthcare system, which hampers integral modernization and a common data base in the sector.

In response to this, the National Plan for the Implementation of Integrated Healthcare Networks was enacted in 2021, providing for transformation of the current organisation of the healthcare system, through the adoption of an integrated healthcare network model.

We anticipate that as the use of healthtech within the healthcare sector develops, there will be more changes to the current legal and regulatory framework, and healthcare regulators.

Claims landscape

Due to the use of technological advancements being relatively new and not widespread in Peru, we are currently not aware of any medical malpractice claims directly relating to emerging areas of healthtech.

However, there have been claims related to the implementation of telemedicine in the health sector, due to:

1. The lack of awareness among citizens about telemedicine offerings.
2. The current telemedicine offerings being limited and insufficient for all citizens.

An important aspect to take into consideration is the implementation of information and communication technology in the complaints system.

In that sense, users currently have several different means to file anonymous claims related to any healthcare provider, including:

- Through the virtual reception desk of the Superintendence of National Health (SUSALUD)
- A mobile application SUSALUD CONTIGO.
- Social media accounts used by SUSALUD.

It is important to focus the discussion on the adaptation of concepts of liability, including limitations, burden of proof, and the attribution of liability to the developers of technology. If traditional concepts of liability prevail, exposure of healthcare professionals may be larger for matters beyond their control.

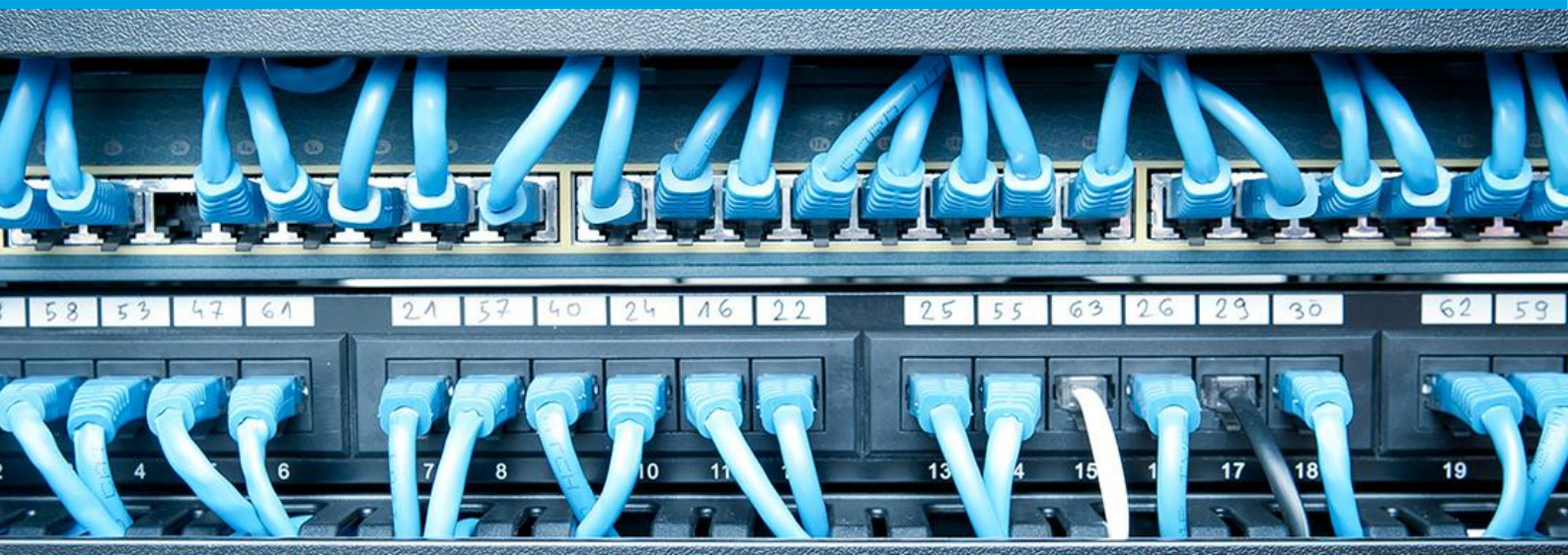
Securing adequate insurance providing coverage for professional liability when technological developments are in place, will be particularly important.

We anticipate the relationship between patients and healthcare professionals will most likely be challenged as the use of healthtech within the healthcare sector develops in Peru.

Contact

Fernando Hurtado de Mendoza
Partner, Lima
e fernando.hurtadodemendoza@kennedyslaw.com

Cyber risk and data privacy:
The healthcare perspective



Cyber risk and data privacy: The healthcare perspective

Cyber incidents and data breaches continue to be a major concern for the healthcare sector globally.

> **Statistics from various countries consistently show that the healthcare sector has more data breaches than any other industry sector, and that those data breaches are consistently more costly than any other industry sector.**

In Australia, the healthcare sector accounted for 18% of all data breaches notified to the Office of the Australian Information Commissioner in 2021. It has been the industry sector with the highest number of data breaches in every reporting period since the Australian notifiable data breaches scheme began in 2018.12

In the US, the Identity Theft Resource Center reports that the healthcare sector experienced 330 data breaches in 2021. Again, this was more than any other sector, and more than 28 million individuals were affected by those breaches, second only to the utilities industry.[13]

In its annual survey of the costs of data breaches, the Ponemon Institute found that the average total cost for a data breach in the healthcare industry was US$9.23 million. This was almost double the cost of a breach in the financial services industry, which ranked second.[14]

Why does the healthcare industry suffer so many data breaches?

The healthcare industry is prone to data breaches, and particularly expensive data breaches, for several reasons.

Firstly, the healthcare industry handles a large volume of sensitive and valuable personal data. Health records are obviously highly sensitive, and can be valuable on the black market or used for the purposes of extortion. The healthcare industry also holds a range of government identifiers and financial details, which can be used for identity theft. IT systems of healthcare providers is often critical infrastructure, and therefore attractive as a high-profile target.

Secondly, the healthcare industry continues to have poor security relative to other highly-targeted industry sectors such as financial services and IT. While large, well-funded hospitals may be able to afford robust security, hospitals relying on government funding in countries where there are more limited resources for investment in such security may struggle. Even in countries where greater investment in cyber security is made, the industry includes many smaller clinics and individual practitioners who may lack the expertise to protect their data.

Thirdly, in many countries, the healthcare industry still has a relatively heavy reliance on the manual sharing of health records. Paper health records are still common in many countries, and are often shared between practitioners by unsecure methods, such as fax or email.

Statistics show that the healthcare industry is the only industry sector in which data breaches are more often caused by human error than by malicious actions.

Finally, healthcare providers tend to use a relatively wide variety of small networked devices – wearables, sensors and tablets. These kinds of small devices allow the monitoring of patient health and for doctors and nurses to access data while moving around a hospital. However, because of their size and simplicity, these devices often have relatively basic security features and support compared to the servers and workstations that form the IT networks of many other businesses.

A large number and variety of devices also means many potential points of entry for threat actors.

Recent high profile incidents

A review of several recent high profile incidents in the healthcare industry illustrates the range of different types of incidents.

Ransomware attacks have become increasingly common across all industries over the past two years, and they are particularly disruptive to healthcare facilities. Eastern Health, which operates four major hospitals in the eastern suburbs of Melbourne, suffered a ransomware attack in March 2021.[15] Staff were unable to access patient records and other systems, such as email, for several weeks. While emergency surgeries continued, category two surgeries (surgeries which could wait up to 90 days) and below were postponed for a month due to a lack of patient medical history data.

Ransomware attacks can also affect the healthcare industry through their effect on upstream service providers.

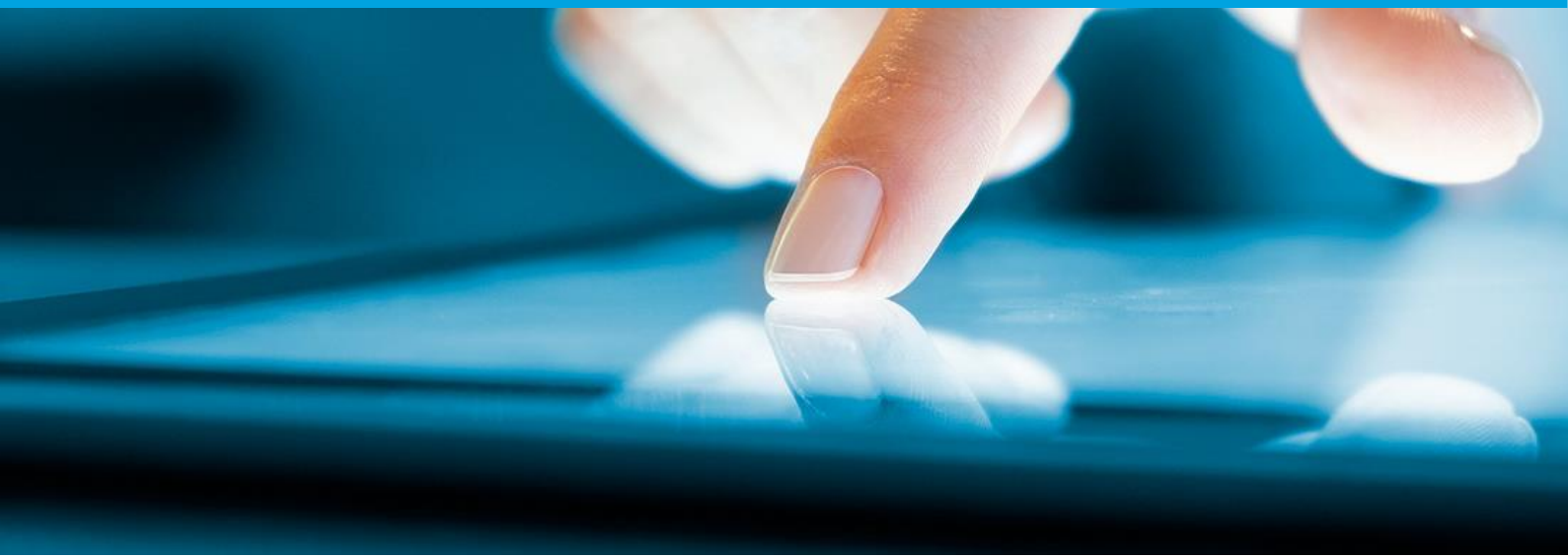
In April 2021, a manufacturer of radiation treatment equipment suffered a ransomware attack, which meant that patient data stored on the manufacturer's servers became unavailable for 18 days. The outage impacted 170 hospitals across the USA, and radiation treatment of hundreds of thousands of cancer patients had to be paused.

Another example of this was the hack of the Accellion file transfer application in January 2021. While the hack impacted companies across all industry sectors, the healthcare sector saw the largest number of those affected.

The breach of Banner Health in 2016 demonstrated the challenges of securing the IT infrastructure of a large hospital. In that case, hackers infiltrated the payment processing system used in Banner's hospital cafeterias, which they then used as a gateway into Banner's main network.[16] They were able to access the data of 3.7 million patients, doctors, employees, health insurance policyholders and cafeteria customers.

A class-action lawsuit in relation to the incident settled for US$8.9 million in 2020, and a regulatory investigation in relation to the incident concluded in 2021 and resulted in orders for Banner Health to take corrective action and pay a fine of US$200,000.

Finally, an incident from the UK demonstrates the potential for patient data to be used for extortion. In December 2020, hacker group 'REvil' stole 900GB of data from IT systems of a UK cosmetic surgery chain, Transform Hospital



Group.[17] The data included photographs before and after procedures. The hackers threatened to release the photographs if a ransom was not paid, although it is unclear whether they followed through with this threat.

Mitigating against cyber risk

Mitigating against the risk of data breaches requires a mix of both technological and operational measures.

From a technology perspective, there are a number of measures which can drastically reduce the risks of a data breach and the severity if one occurs. These include:

- The use of encryption
- Multifactor authentication
- Security analytics tools
- Data classification schema

From an organisational perspective, it is important to ensure that the organisation is prepared to respond to an incident. Every healthcare provider should have a cyber incident response, which sets out how the organisation will respond to an incident and who will be responsible for the various elements of that response.

Employee training is critical, both to reduce the likelihood of data breaches caused by human error, and to ensure staff know the signs of malicious activity.

Finally, healthcare organisations should ensure they have cyber insurance – insurers not only cover their policyholders for the costs associated with responding to an incident, but will usually appoint experts to assist in conducting the incident response.

Contact

Nicholas Blackmore
Special Counsel, Melbourne
t +61 3 9498 6602
e nicholas.blackmore@kennedyslaw.com

References

[1] Recently, the World Index of Healthcare Innovation ranked Australia 19th out of 31 countries for Science & Technology *freopp.org/australia-freopp-world-index-of-healthcare-innovation-4c6c401af0fc*

[2] Stefan Hajkowicz et al, 'Artificial intelligence: Solving problems, growing the economy and improving our quality of life' (Report, CSIRO Data61, 2019) 29 *data61.csiro.au/~/media/D61/AI-Roadmap-assets/19-00346_DATA61_REPORT_AI-Roadmap_WEB_191111.pdf?la=en&hash=58386288921D9C21EC8C4861CDFD863F1FBCD457*

[3] Kate McBride et al, 'Detailed cost of robotic-assisted surgery in the Australian public health sector: from implementation to a multi-specialty caseload' (2021) 108 *BMC Health Services Research* 1, 1 *bmchealthservres.biomedcentral.com/track/pdf/10.1186/s12913-021-06105-z.pdf*

[4] Denham Sadler, *Regulators must step up on AI medical products* (24 November 2020) InnovationAus *innovationaus.com/regulators-must-step-up-on-ai-medical-products*

[5] Joseph Sung, Cameron Stewart and Ben Freedman, 'Artificial intelligence in health care preparing for fifth industrial revolution'(2020) 213(6) *The Medical Journal of Australia* 253, 255 *mja.com.au/journal/2020/213/6/artificial-intelligence-health-care-preparing-fifth-industrial-revolution*

[6] Miki Wada et al, 'Use of artificial intelligence in skin cancer diagnosis and management' (2020) 213(6) *The Medical Journal of Australia* 256, 259 *mja.com.au/system/files/issues/213_06/mja250759.pdf*

[7] Australian Health Ministers Advisory Council, 'National health genomics policy framework 2018-2021' (Commonwealth Department of Health, 2017) 2 *health.gov.au/internet/main/publishing.nsf/Content/national-health-genomics-policy-framework-2018-2021*

[8] Jane Tiller and Margaret Otlowski, *Can (and should) a doctor tell my biological relative my genetic results without my consent* (13 December 2018) The Conversation

[9] Avant Mutual, *A discussion paper: Genomic testing and medico-legal risk* (21 August 2020) Avant Mutual *avant.org.au/WorkArea/DownloadAsset.aspx?id=23622330094*

[10] https://www.fwd.com.hk/en/press/2021/fwd-x-hkt-x-ghk-hypertension-care-programme/

[11] La Biotech, secteur-proue de l'écosystème startup français ?*maddyness.com/2020/02/06/healthtech-biotech-medtech*

[12] Office of the Australian Information Commissioner Notifiable Data Breaches Report *www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics*

[13] ITRC 2021 Annual Data Breach Report *https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/*

[14] IBM Cost of a Data Breach Report 2021 *https://www.ibm.com/au-en/security/data-breach*

[15] *https://www.theage.com.au/national/victoria/staff-unable-to-access-patient-files-after-eastern-health-cyber-attack-20210329-p57eyj.html*

[16] *https://healthitsecurity.com/news/judge-approves-8.9m-banner-health-settlement-over-2016-data-breach*

[17] *https://www.bbc.com/news/technology-55439190*