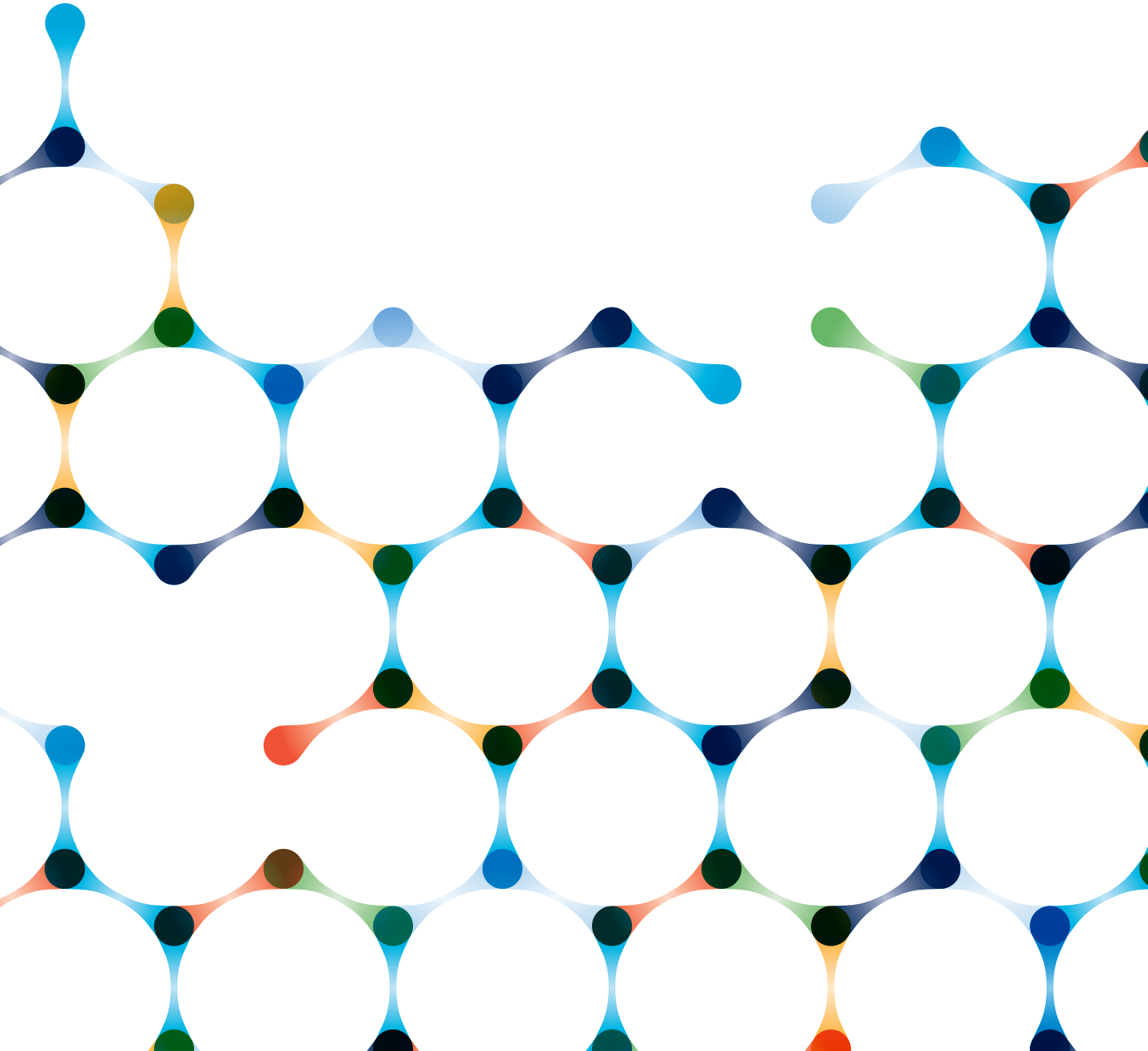
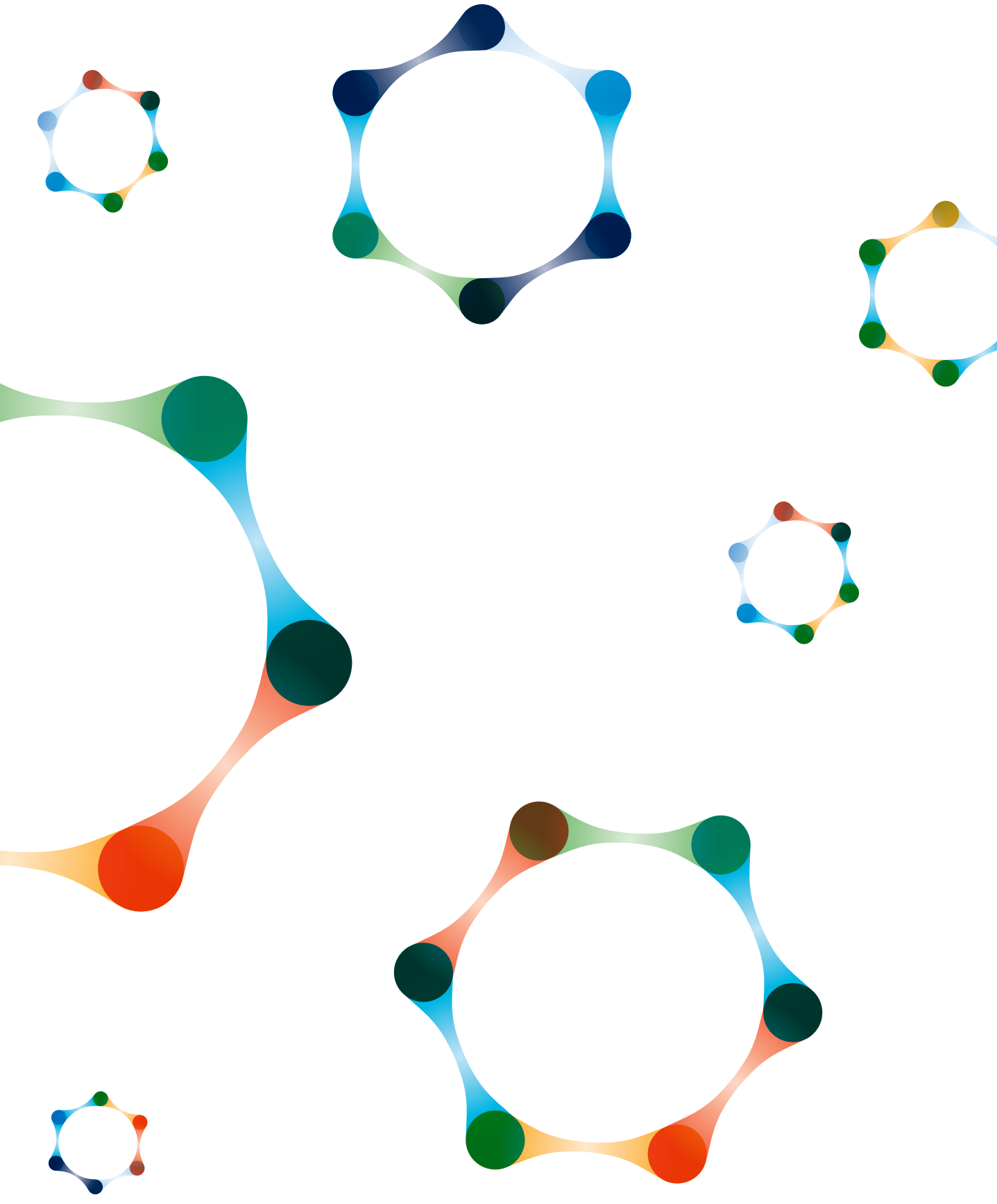
Freshfields Bruckhaus Deringer

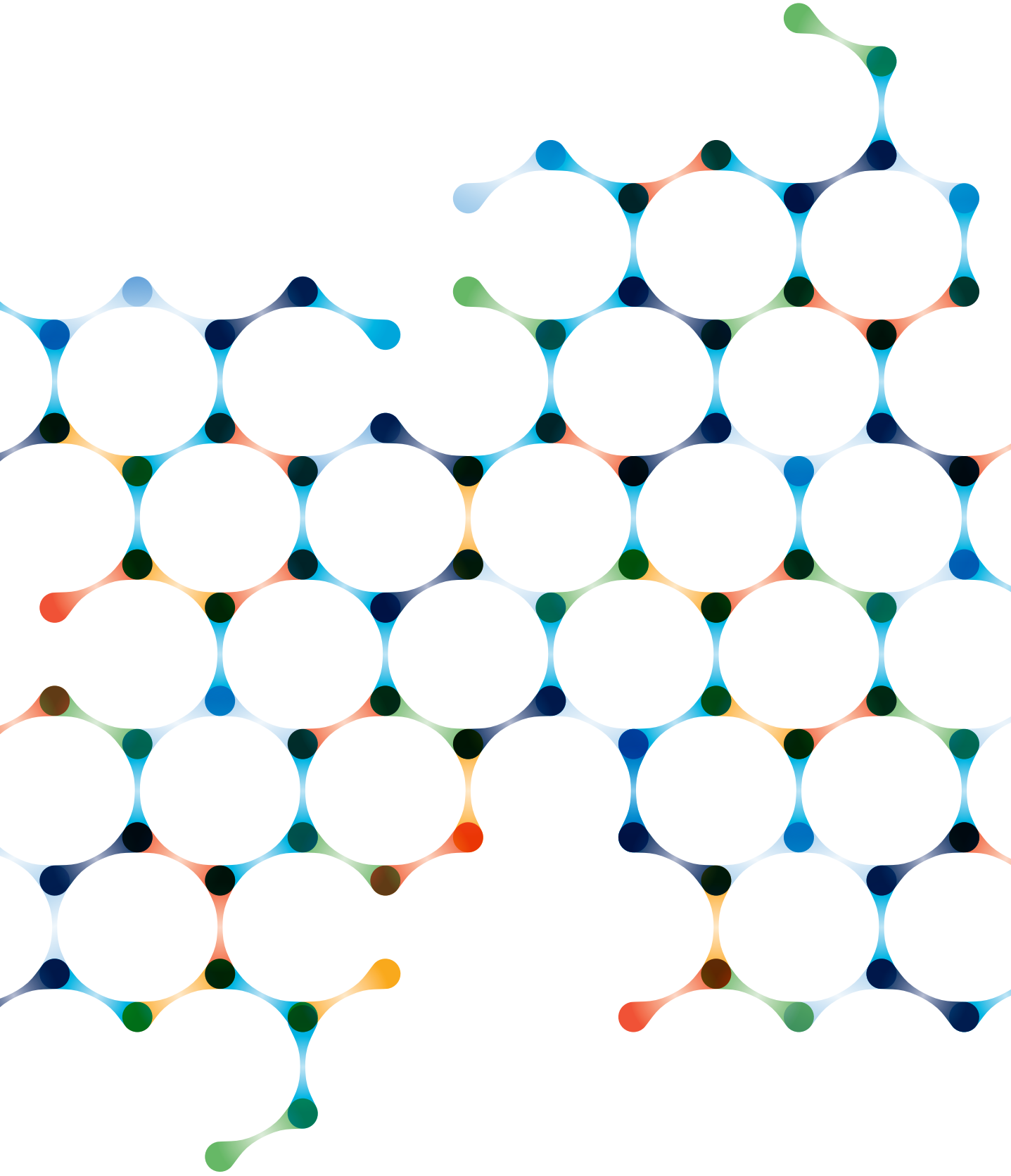
eHealth

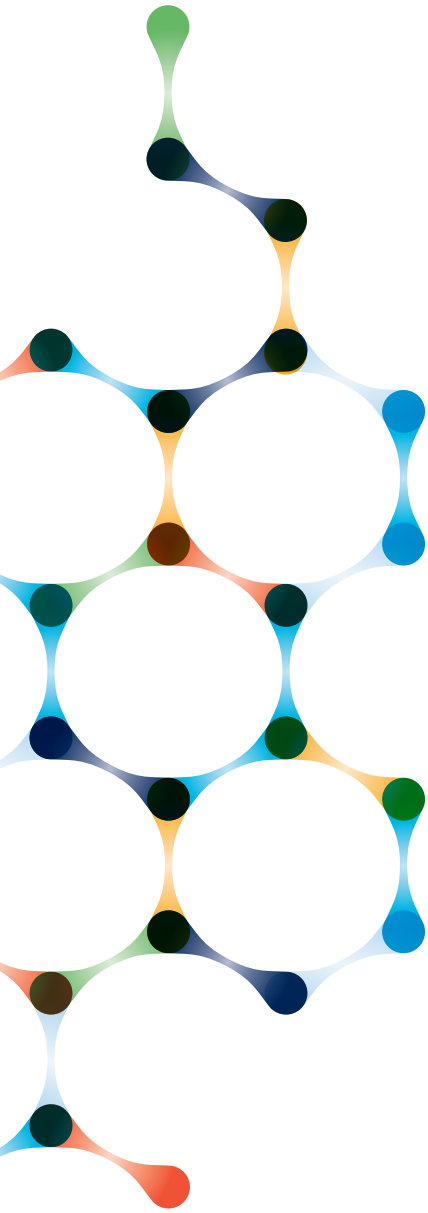
The issues that matter





Contents





Both eHealth and mHealth widen the scope for better healthcare. eHealth and mHealth products and solutions will improve the management of patient treatment and the way physicians communicate with patients and each other, both within and outside clinical settings. They will empower patients to take more control over their own health and healthcare. These products and services also raise novel issues around regulation, liability, data privacy, cyber security and more. While answers to questions in these areas are in flux, you should prepare now for the issues you are likely to face.

Here, we touch on some of the most important issues and why they matter.

Technology outpacing regulation

Governments and regulators have begun to address whether current regulations cover eHealth. Many have yet to finalise their positions.

In the European Union

The EU regime offers little clarity between apps that are medical devices and apps that monitor lifestyle and wellbeing. In the absence of clear guidance, there will be many borderline cases. For example, are wellbeing apps that allow users to chart weight loss over time properly classifiable as medical devices? Or does the regime only cover more sophisticated apps, such as those that tell diabetics when and in what doses to take medicine? It may not always be obvious whether your product will be classified as a medical device or not.

The way in which an app or device is regulated can have a 360° effect on your business model. If you make and sell medical devices, you must adhere to medical device regulations, as well as to onerous validation and testing requirements.

Medical devices are also subject to CE marking and conformity assessments in the EU.

In the US

The Food and Drug Administration's (FDA) approach is to balance encouraging innovation with managing the risks. Recognising the potential benefits to public health, the FDA has elected for the time being not to apply its oversight to many mobile apps and lifestyle/wellness products. Apps that will however be regulated include those used in active patient monitoring or analysing patient-specific medical device data from a connected device.

In China

The Chinese market has an evolving but as-yet-undeveloped regulatory framework. China has issued only three (interim) licences for online sales of over-the-counter drugs to date. Online sales of prescription drugs are not permitted, but this is expected to change in 2016.

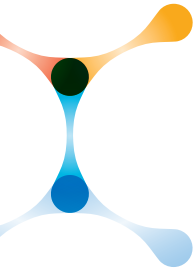
Telemedicine is not regulated, but the National Health and Family Planning Commission has published binding guidelines to remove medical services provided by a hospital, though these have yet to be brought into effect.

Chinese law is currently silent on mobile medical apps. The borderline between apps that are medical devices and those that are lifestyle and wellbeing apps remains undefined.

Why this matters

A new medical devices regulation is expected in the EU in late 2015. We expect the FDA's guidance will also evolve over time. In addition, lots of uncertainty exists in China as regulations still have a long way to develop. All this makes it vital that you continually monitor your products against prevailing rules and adopt a prudent risk-mitigation approach in the absence of specific rules in many areas.

> It may not always be obvious whether your products will be classified as a medical device.



A new frontier for data privacy

The European Data Protection Supervisor has said that she will regard data from lifestyle and wellbeing apps to be health data when processed in a medical context.

The European Data Protection Supervisor (EDPS) published a report on mHealth on 21 May 2015. In reconciling technological innovation with data protection she said that she was particularly concerned about information asymmetry and the need for meaningful consents. Consumers do not read lengthy data collection statements and do not really know what data is being collected about them and how it is being used. The EDPS also warned against the use of big data in the mHealth industry for harmful practices against individuals, such as discriminatory profiling, and maintained that big data usage should be strictly for purposes that are beneficial to the individuals.

Therefore, we expect renewed emphasis on data minimisation and whether bundled consents to data usage are a valid approach in this sensitive area of health data. This will lead to more demands for transparency about exactly what data you are collecting and for what purpose. The way you get consent is also likely to be scrutinised, even beyond the EU. And this will create practical concerns about how you provide consent information on a small-screen, mobile device.

Consent collection will need to be revisited to avoid potential violations. Standardised general terms and conditions in the eHealth and mHealth context are unlikely to work.

The new high watermark

The EU is currently discussing a new data privacy regulation. Consent to process personal data — not limited to health data — will need to be unambiguous, explicit, voluntary and revocable. The latest draft of the regulation, from June 2015, would allow EU data protection authorities to impose fines of up to €1m or 2 per cent of worldwide annual group turnover. The Council has agreed to enact the regulation by the end of 2015 — so it could take effect in late 2017.

This could affect you as a vendor of health apps wherever you are, as the proposals may be extended to data controllers and processors that operate in the EU, regardless of where the data is processed.

Managing cross-border transfers

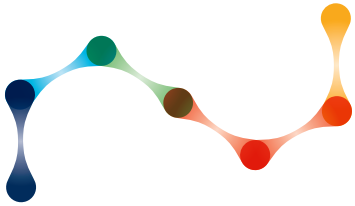
Apps and wearable devices could, in principle, collect data from anywhere in the world, with data that is not stored locally often being processed at a central collection point in a different country from the user. Transferring sensitive information from the EU to recipients in countries without adequate data protection is, in general, prohibited. And transferring sensitive personal data outside of almost any country requires consideration of often highly complicated rules.

Such issues create practical compliance obstacles that you may need to work through, depending on where you collect and process data. The EDPS, for example, has stated her strong preference for data to be processed locally — on a device — rather than to be transferred for remote processing on a centralised platform.

Why this matters

These are many signs that data privacy regulators are taking more interest in eHealth, which is likely to presage heightened levels of enforcement and new stronger enforcement measures. Companies will need to find ways to balance the trust equation.

> Transferring sensitive personal data outside of almost any country requires consideration of often highly complicated rules.

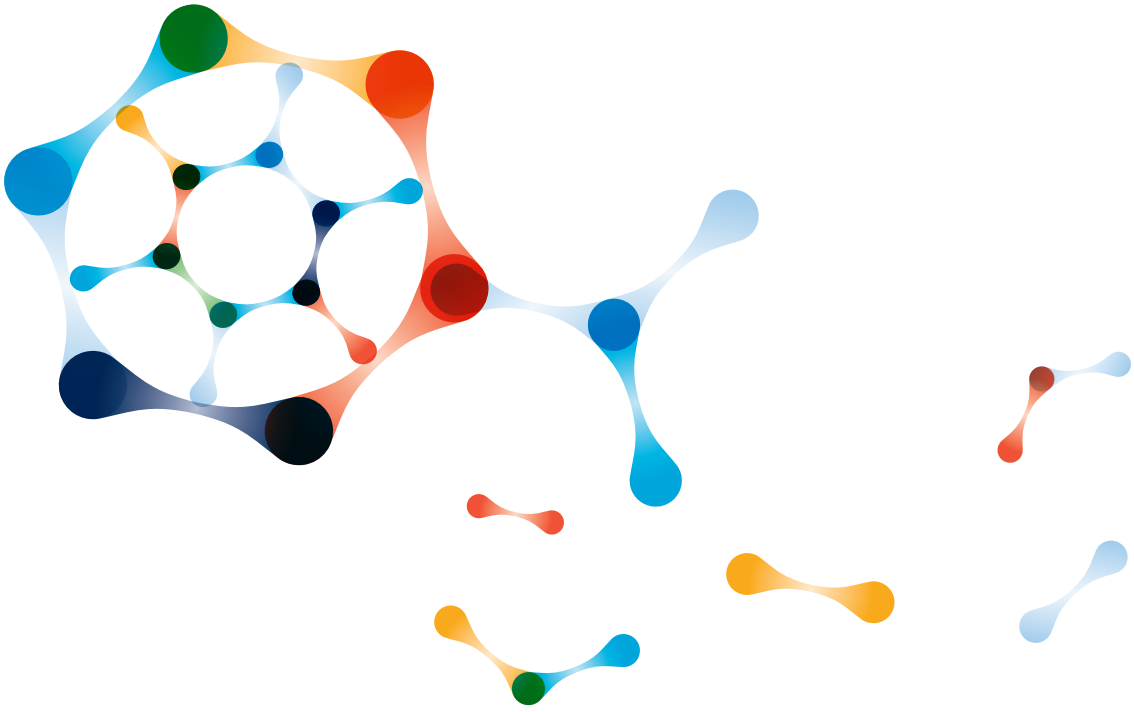


Product liability and jurisdictional issues

Compliance with a wide variety of stringent product liability laws around the world poses a significant challenge to providers of novel eHealth technology.

As the provider of an app that transforms a mobile phone into a medical device, you could owe a duty of care both to the healthcare provider that relies on data from the app or uses the device to provide treatment and to patients themselves. A doctor or other healthcare professional will typically be expected to exercise independent judgement in filtering and applying diagnostic information that an app provides. However, eHealth and mHealth may also bring about a reduced involvement by physicians and greater autonomy to patients. This gives rise to a range of new opportunities, but also requires producers to mitigate against the greater risk of harm.

Unpicking these situations among multiple operators and intermediaries to attribute responsibility for an incorrect diagnosis or treatment will test the boundaries of existing product liability laws in many jurisdictions, particularly in circumstances where eHealth services are provided across borders.



How product liability laws work

The Product Liability Directive in the EU imposes a no-fault liability regime. As a manufacturer or importer, you may be liable if a product 'defect' harms an individual or damages property. There is no need for the user to prove that you were at fault or failed to take suitable precautions.

Even if you are able to establish that all reasonable precautions were taken, this is not a defence. This makes pre-market testing and ongoing monitoring essential to pre-empt defects and prevent harm from occurring. A consumer may bring a claim in negligence. This risk may also be mitigated by stringent testing and oversight. However, the complex and novel nature of many eHealth technologies may require an innovative approach. Claims may also be possible in contract.

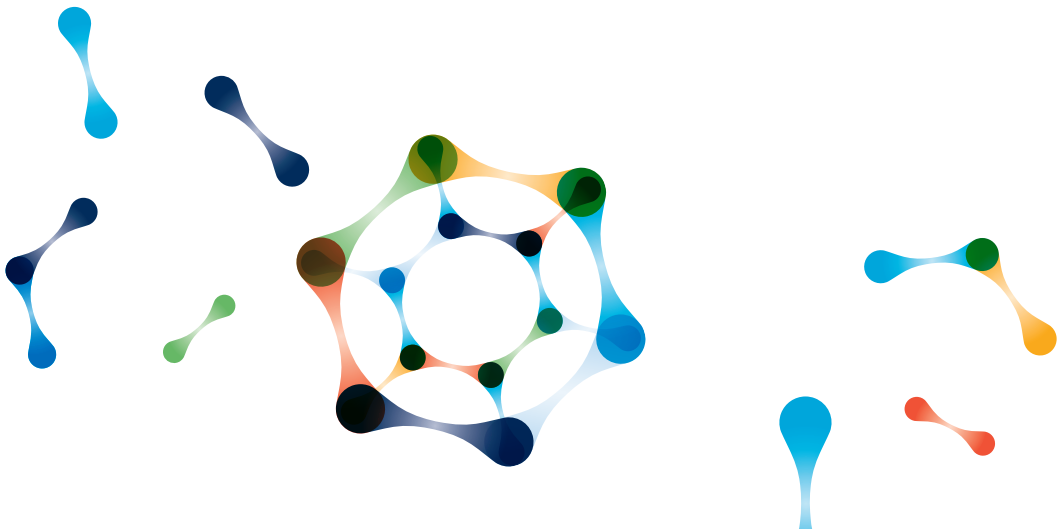
Consumer protection legislation often limits the extent to which you may exempt yourself from liability for loss or damage caused by negligence or arising from a breach of mandatory terms under sale of goods or supply of services laws. In many cases, liability for death or personal injury resulting from negligence can be neither excluded nor limited, while legislation also restricts limitations of liability for other negligent acts. It is necessary to understand how these laws may affect your liability.

Jurisdiction and governing law

The introduction of eHealth devices also raises jurisdictional issues. Medical advice provided remotely via an app could potentially be accessed in any country. Healthcare advice provided from Germany, therefore, could be accessed in Russia, making it unclear whose laws will govern the treatment. In cases where something goes wrong, claimants are likely to forum shop, pursuing claims in jurisdictions where consumer protection laws are stricter and/or damages rules more generous (eg in the US). This makes it important to have a detailed understanding of potential markets and the legal challenges they may pose.

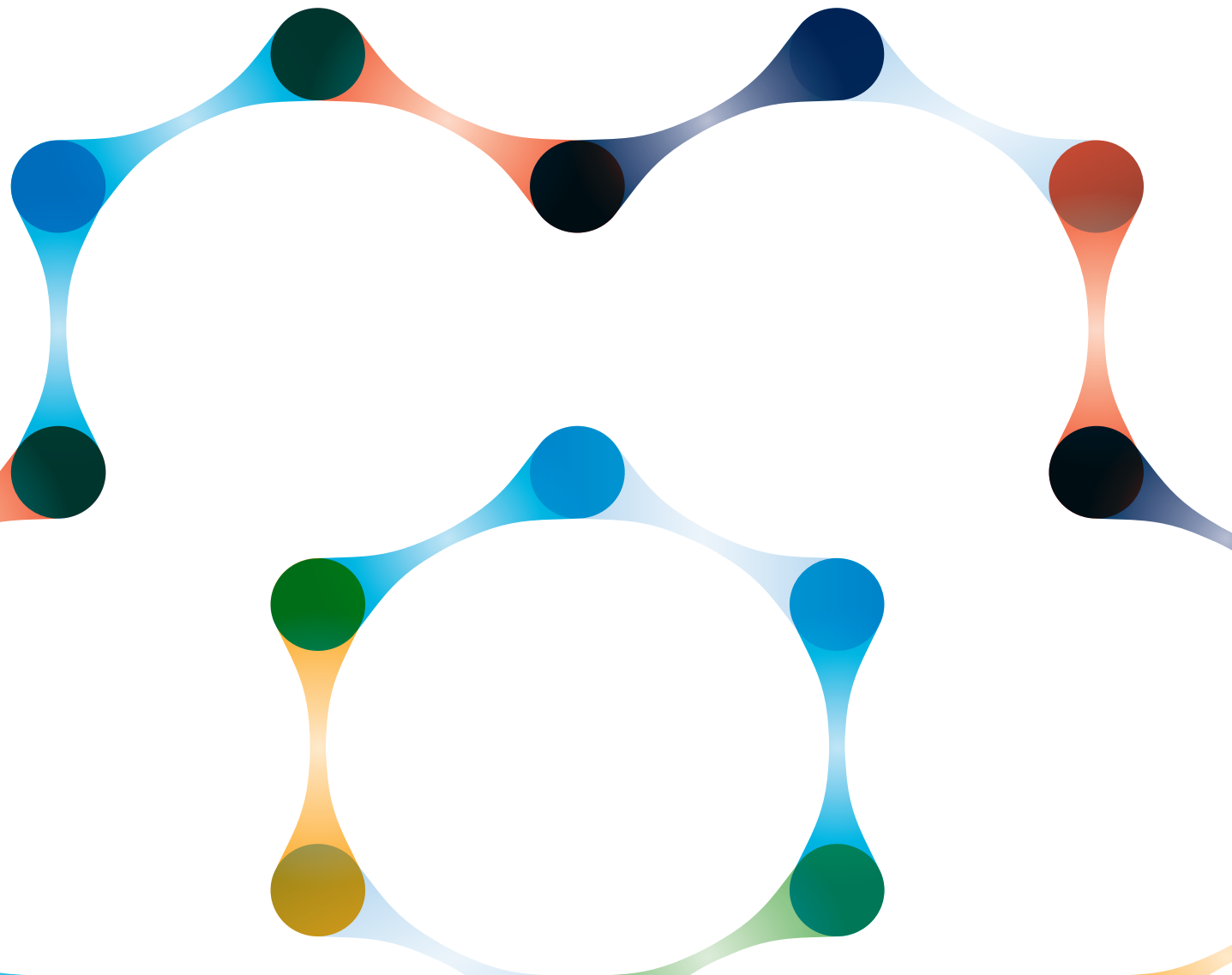
Why this matters

This, and similar issues, remain unresolved in many countries. Liability regimes for healthcare professionals vary from country to country and between EU member states. It is therefore vital to ensure proper compliance and comprehensive oversight, coupled with appropriate contractual protections.



Cyber security rules ‘under observation’

Cyber attacks on insured healthcare organisations have increased roughly 125 per cent over the last five years, and the fallout could be costing the healthcare industry $6bn a year.



Anthem, a health insurer in the US, suffered a cyber attack in February 2015 that was one of the largest witnessed to date in terms of data loss. The details of roughly 80 million patients — from names to social security numbers — were stolen, though no medical data was included. It was reported that notifying affected patients could use up most of Anthem's cyber insurance. State attorneys and the FBI are also investigating the attack, its consequences and Anthem's responses.

Since then, three other US health insurers have had customer records hacked into.

Legislation has been slow in coming

In the US, President Obama signed executive orders in 2013 and February 2015, after earlier legislative proposals failed to pass Congress. These orders were to allow agencies to share classified cyber security information with companies to improve security systems.

In the EU, a cyber security directive has been in development since 2013. The draft directive proposes mandatory breach-notification requirements and increased baseline security standards that would also be passed on to suppliers.

Regulators lead the charge

In October 2014, the FDA issued guidance on cyber security measures for medical devices and recommended disclosures in the pre-market submissions. The guidance applies to all devices that contain software and to all software that constitutes a medical device.

As a device maker, your pre-market submissions to the FDA should describe and justify the security measures you have adopted. The FDA advises that you address security during the design and development of devices and establish a vulnerability and impact assessment matrix.

There are few specific cyber security standards for medical devices in Europe. But regulators generally consider that all health data should be encrypted during both storage and transit. France, in fact, requires cloud providers to certify that they have adequate security before they are permitted to store health data.

Why this matters

Regulators may intervene further. This could include mandatory testing and validation requirements for cyber security measures in higher-risk apps and devices classified as medical devices. There are also indications that the European Commission may favour mandatory certification of encryption and other security measures in some situations.

details* of
±80m
patients
were stolen

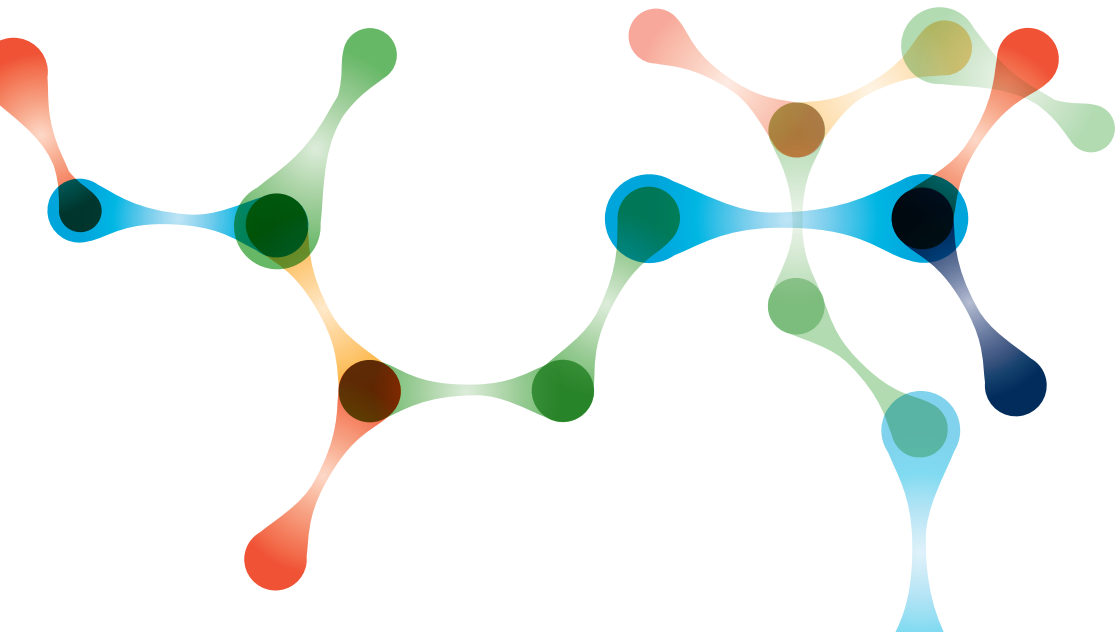
**including names and social security numbers (but not medical data)*

The experience that matters

Digitalising healthcare-related services offers enormous scope for innovation and cost savings in healthcare provision. It also creates challenging new legal issues.

As a digital convergence industry, many successful eHealth ventures will be founded on partnerships: partnerships between pharma companies, tech companies, specialist software providers, insurance companies, telcos and other healthcare incumbents, as each looks to access expertise outside its traditional core strength. Each participant will be required to operate across the boundaries of its traditional business, encountering unfamiliar legal and regulatory risk. To succeed will require a multidisciplinary approach.

Similarly, Freshfields' eHealth team has brought together lawyers from across the firm, in the fields of medical regulation, data privacy, product liability and medical negligence, intellectual property and cyber security, and from both our consumer and healthcare and our TMT sector groups. Working together, we provide a 360° view of any issue in this emerging field.



Your Freshfields contacts

Andrew Austin
Partner
T +44 20 7716 4048
E andrew.austin@freshfields.com

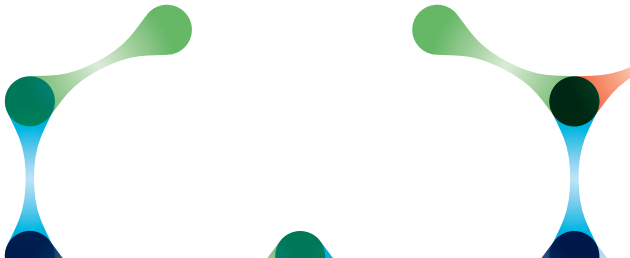
Daniel Cendan
Counsel
T +1 212 277 4019
E daniel.cendan@freshfields.com

Jennifer Bethlehem
Partner
T +44 20 7716 3058
E jennifer.bethlehem@freshfields.com

Jochen Dieselhorst
Partner
T +49 40 36 90 63 18
E jochen.dieselhorst@freshfields.com

Richard Bird
Partner
T +852 2913 2660
E richard.bird@freshfields.com

Marcel Kaufmann
Partner
T +49 30 20 28 37 43
E marcel.kaufmann@freshfields.com



freshfields.com