DAC BEACHCROFT

DIGITAL HEALTH INSIGHTS

10 key legal considerations when developing a health app

The pace of adoption of technology across the health and care sector has continued to grow post-pandemic. Health apps, such as those providing telemedicine, self-management of health conditions and wellbeing support, can play an important role in improving patient outcomes. We have set out 10 key legal considerations when developing a health app for use in the United Kingdom.

1. APPLICABLE REGULATORY FRAMEWORKS

In the UK, there is no specific regulatory framework for health apps or telemedicine and the relevant regulator(s) ultimately depends on the functionality of the app and any associated services being provided. Some of the key regulators of the UK health and care sector that may be relevant to ensuring regulatory compliance of your health app are:

- the Care Quality Commission ("**CQC**"), which regulates health and care providers;
- the General Medical Council ("**GMC**") and other professional regulators that regulate individual health and care professionals;
- the Medicines and Healthcare products Regulatory Agency ("**MHRA**") which regulates medical devices, including software as a medical device; and
- the Information Commissioner's Office ("**ICO**"), the body responsible for upholding information rights.

It is essential to understand:

- what services and products are being provided through your app and to whom?
- what regulatory requirements are applicable and how to comply with the same?

Given the pace of proliferation of health apps, the regulatory requirements are also evolving seeking to keep up. For example:

- in May 2022, the CQC updated its "Scope of Registration" guidance with new provisions relevant to the regulation of AI software, and how remote provision of services under the regulated activity of "Transport services, triage and medical advice provided remotely". In 2021, the MHRA announced that it was planning to regulate software devices by a series of 'work packages' and in October 2022, the MHRA issued guidance "Software and AI as a Medical Device Change Programme – Roadmap" summarising these work packages. We have explored this in more detail in our briefing on the roadmap.

2. RISK ALLOCATION AND LIABILITY

Ascertaining liability for the products and/or services provided through your app is critical, not only from a potential regulatory perspective but also so this is clear to users.

For example, if your app involves the provision of clinical services, consider who is responsible for this care. If a third party is responsible for the care, have you carried out due diligence to confirm they have the relevant registrations and licences and incorporated appropriate obligations into contractual arrangements, such as a requirement to maintain and evidence the registrations and licences?

Liability for the products and/or services should be clearly articulated to users in the terms of use for your app ("**Terms of Use**").

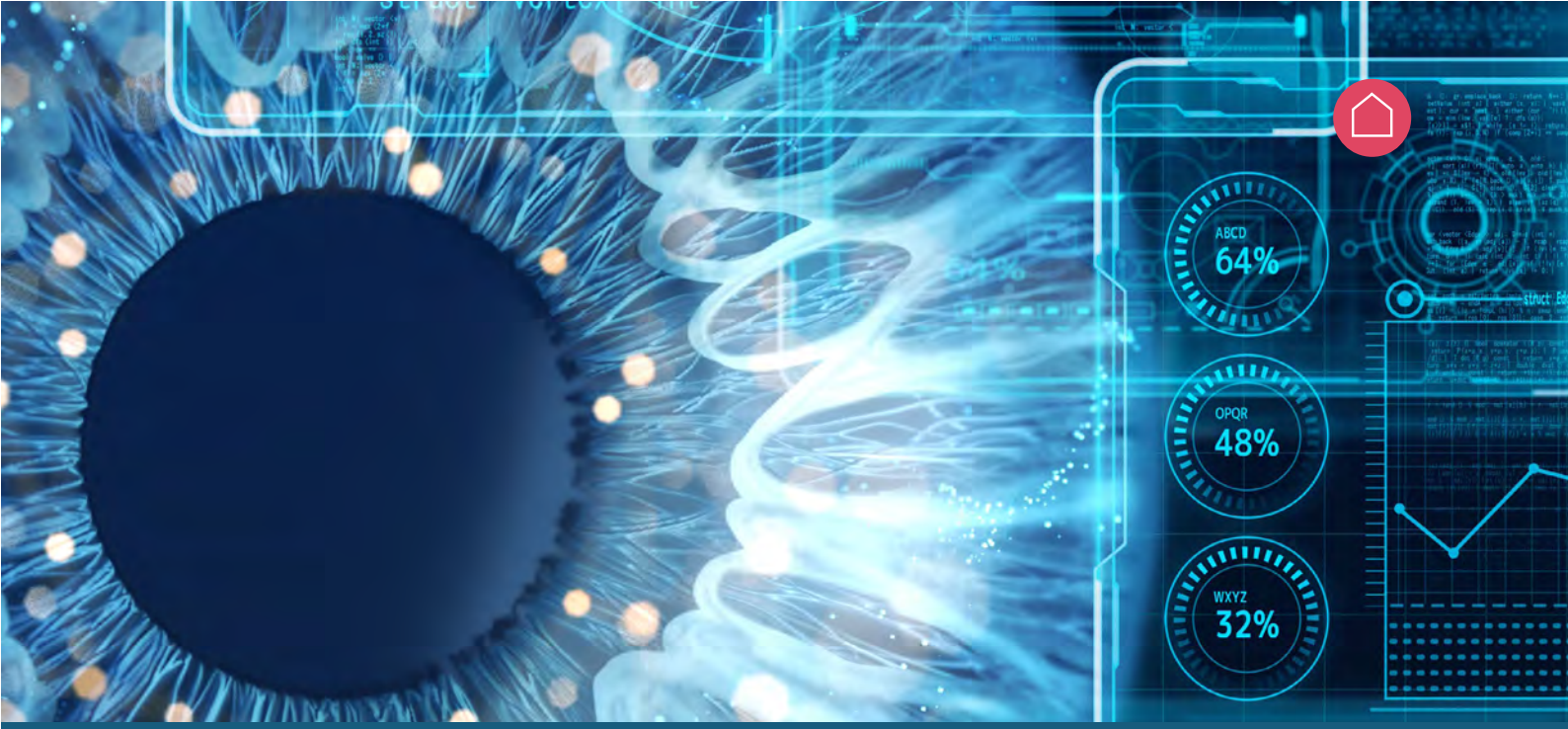
3. SOFTWARE AS A MEDICAL DEVICE

The UK Medical Devices Regulations 2002 (SI 2002/618, as amended) regulates medical devices in the UK. The UK regime is subject to reform and new regulations are anticipated by July 2024, where we will likely see an expansion of what falls within the definition of software as a medical device. It is expected that the majority of change required in the area of software as a medical device will be in the form of guidance. Legislation setting out transitional arrangements is expected in spring 2023.

All medical devices must be registered with the MHRA before being placed on the market in Great Britain. The MHRA is the competent authority responsible for the UK medical device market.

The MHRA has produced guidance on when software applications are considered to be medical devices and it is the responsibility of the manufacturer to determine the classification. Monitoring of fitness/health/well-being is not usually considered to be a medical purpose. Decision support software is likely to be a medical device if it is linked to a specific medicine/device, is intended to influence treatment or results in a diagnosis or prognosis.

Careful consideration should be given and advice sought on whether your health app is, in whole or in part, a medical device.



4. USING YOUR APP OUTSIDE OF THE UNITED KINGDOM

Consider where the products and/or services that your app offers can be accessed from and whether you wish to impose limitations or restrictions on users being able to access the app when they are located (either permanently or on a temporary basis) outside of the UK.

If your app is intended for use outside of the UK, you should ensure it meets the relevant legal and regulatory requirements of those jurisdictions.

For example, providers of remote medical advice should consider whether remote consultations are available when users are abroad (temporarily or permanently) and whether there are any limitations such as on issuing prescriptions when individuals are outside of the UK.

If your app is intended for use only in the UK, or if there are any other territorial restrictions or limitations, make sure this is clear to users in the Terms of Use.

The impact of transferring personal data outside the UK is considered further in the section on data protection below.

5. PROTECTING YOUR INTELLECTUAL PROPERTY ("IP") RIGHTS

The app's Terms of Use should be clear as to who owns the IP in the app and what rights the users have to use the material in the app. For example, the Terms of Use should set out that IP rights in the app belong to you and/or your licensors and include a limited licence for the user to use the material. It is advisable that technical measures are put in place to prevent the copying of material from your app.

If you are working with third parties in connection with your app, it will be important to ensure that your contractual arrangements with them protect your IP rights. For example, if you are using third party software developers, you will need to ensure you have the requisite rights to use the IP they create for you. Protection of your IP will be of fundamental importance to the value of any health app.

6. COMPLIANCE WITH CONSUMER LAW

When providing goods, services and/or digital content through an app to a consumer, you will need to ensure compliance with consumer rights law, including:

- **Consumer Rights Act 2015**-in-scope services, goods and digital content must be of satisfactory quality, fit for a particular purpose and as described; and
- **Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (SI 2013/3134)** – these regulations set out, amongst other things, pre-contract information requirements and cancellation rights in respect of in-scope services, goods and digital content.

7. COMPLIANCE WITH ADVERTISING LAW AND STANDARDS

There are specific rules in the UK (and complementary regimes across Europe) for the advertising of medicines, medical devices, treatments, health-related products, which supplement the general requirements under the Advertising Standards Authority ("ASA") and Committee of Advertising Practice ("CAP") Code. Different requirements apply depending on whether the intended audience is the general public or healthcare professionals.

In particular, health app providers should ensure compliance with relevant provisions of the CAP Code (Rule 12).

Adverts (which includes content on an app provider's own website) should be legal, decent and truthful. In addition, for health-related apps, any advertising must:

- ensure any objective claims are backed by evidence;
- not discourage essential treatment for conditions for which medical supervision should be sought;
- not offer to provide a diagnosis or suggest a treatment by correspondence;
- not confuse consumers by using unfamiliar scientific words for common conditions;
- in respect of self-diagnosis of minor ailments, not make claims that might lead to a mistaken diagnosis;
- not encourage patients to use a product to excess; and
- not falsely claim that a product or device can cure illness, dysfunction or malformations.

Breach of the CAP Code may result in the publication of ruling against the advertiser and have related reputational consequences.

In addition to the requirements above, the MHRA Blue Guide provides guidance on the legal requirements for medicines advertising in the UK. You should familiarise yourself with the MHRA Blue Guide if promoting or advertising your app means you are promoting and advertising medicines.

8. DATA PROTECTION

If your app collects and otherwise uses personal data (to mean information from which an individual can be identified) then data protection laws will apply. The location of that processing will determine the applicable laws, for instance if it is confined to the UK then it will fall within the remit of UK data protection law but equally if that data is transferred to the EU or beyond then local laws will also apply.

Key data protection considerations for app developers include:

- complying with the principle of data protection by design and by default, which means that you should develop the functionality of your app with any relevant restrictions or obligations in mind so as to ensure they are adequately addressed;
- mapping out relevant data to be collected and used by the app, to include whether any special category data, such as data concerning health, will be used by the app (as that gives rise to additional compliance obligations?
- ensuring that you are able to lawfully use the data as you intend, by reference to the possible legal justifications for data use (also referred to as 'conditions for processing) available under the UK GDPR. Particular attention should be paid to any intended marketing activities, which are likely to require consent.
- complying with the principle of transparency, by providing individuals who use the app with a clear, detailed privacy notice when they first start using it, setting out how their data will be used, who it will be shared with and how they exercise their rights under data protection law.
- giving effect to appropriate technical and organisational security measures, which take into account the nature and sensitivity of the data concerned.
- will personal data be transferred outside of the UK and, if so, are adequate protections in place? Those protections may be addressed through an adequacy decision by the UK government in favour of the country to which the data is to be transferred (which currently includes all countries within the EU), and in which case no further steps are required. If, however, no such decision is in place then particular contractual clauses must be agreed in order for the transfer to take place.

This is a high level summary of some of the most important considerations from a data protection compliance perspective, but there are many more which must be navigated in order be considered fully compliant. Further detail can be found on the ICO's website, who has published a range of guidance relating to data protection law.

9. CYBER SECURITY MEASURES

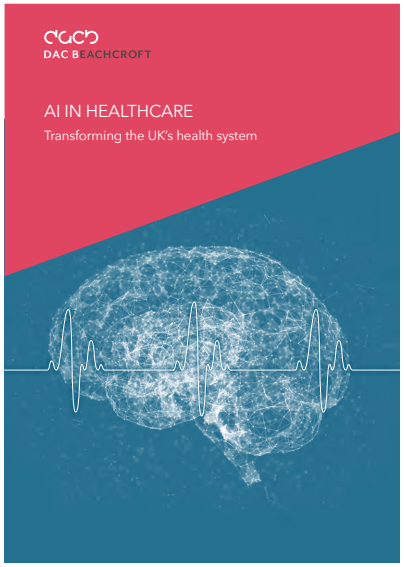
Having robust cyber security measures in place is important for all apps, but particularly health apps holding health data. There should also be systems in place to ensure cyber security measures are periodically checked and updated.

It is advisable to have cyber risk insurance in place to cover the liabilities that may flow from a security breach. Consider the type and level of cover that is appropriate for your app.

10. USE OF ARTIFICIAL INTELLIGENCE IN HEALTH APPS

AI is playing an increasing role in the future of healthcare and the use of AI in health apps gives rise to a number of unique challenges and opportunities. In particular it engages specific considerations as to liability issues, regulatory compliance as well as rights of individuals not to be subjected to decision-making based on automated processing of their data unless particular safeguards are fulfilled. Those issues are explored in depth in our AI in Healthcare – Transforming the UK's Health System report.

Read now



HOW CAN WE HELP?

We have a number of experts in emerging technologies, including AI, with different focuses – tech, regulation, liability, data, etc. We advise many of the UK's and international leading innovators in the digital health space.

We support clients in bringing novel technology from innovation, through design and manufacture, to improve health outcomes for patients. We are expert in understanding the regulatory framework for healthcare operators, medical devices, medicines and more.

OUR TEAM

Hamza Drabu
Partner
Commercial / Regulatory
T: +44 (0) 20 7894 6411
hdrabu@dacbeachcroft.com

Darryn Hale
Partner
Information / Data
T: +44 (0) 20 7894 6125
dahale@dacbeachcroft.com

Emily Broad
Solicitor
Commercial / Regulatory
T: +44 (0) 20 7894 6029
ebroad@dacbeachcroft.com

Kate Loxton
Senior Associate
Intellectual Property
T: +44 (0) 117 918 2398
kloxton@dacbeachcroft.com

Tim Ryan
Partner
Technology / Commercial
T: +44 (0) 207 894 6978
tryan@dacbeachcroft.com

Andrew Allan-Jones
Partner
Intellectual Property
T: +44 (0) 117 918 2251
aallan-jones@dacbeachcroft.com

Alison McAdams
Consultant
Medical Devices Regulation
T: +44 (0) 207 894 6588
amcadams@dacbeachcroft.com

Alistair Cooper
Senior Associate
Technology / Commercial
T: +44 (0) 207 894 6967
acooper@dacbeachcroft.com

Sarah Foster
Senior Associate
Commercial / Regulatory
T: +44 (0) 191 404 4119
sfoster@dacbeachcroft.com

Kelsey Farish
Associate
Technology / Commercial
T: +44 (0) 20 7894 6320
kfarish@dacbeachcroft.com

Louise Kane
Senior Associate
Commercial / Regulatory
T: +44 (0) 20 7894 6556
lkane@dacbeachcroft.com

Becky Daley
Solicitor
Information / Data
T: +44 (0) 20 7894 6033
bdaley@dacbeachcroft.com

dacbeachcroft.com

Follow us: @dacbeachcroft @healthlawuk

Connect with us: DAC Beachcroft LLP