Browne Jacobson

Health care apps - part 2 of 2: delving into data confidentiality

How to protect confidentiality of data by putting in place proper contractual arrangements, setting out how a party may use any information or data associated with the App during its development and prior to it being made available on the market.

04 December 2020

The adoption of smart technology solutions by the health and care sector has exploded in 2020. The pandemic has driven the sector to increase its use of smart phone technology solutions ("Apps"), an example of which is conducting video consultations and assessments. Adoption has historically been slow to develop across the sector generally, potentially due to perceived risks in maintaining integrity of special category personal data.

Now that more health and care providers are transitioning to greater use of Apps, the Covid-19 pandemic has propelled providers to implement systems which can assess an individual's needs remotely.

In the 'new normal', the sector will increasingly adopt and implement the use of Apps to assess and deliver person-centric health and well-being advice and services. The Apps which are created will be in demand, competition is likely to be high and the potential commercial value to providers is significant.

Apps are created by combining software with data (in its broadest sense and by use of personal data). Part 1 of this 2-part series explored how intellectual property rights in Apps might be protected commercially. Part 2 will delve into how to protect confidentiality of data by putting in place proper contractual arrangements which set out how a party may use any information or data associated with the App during its development and prior to it being made available on the market.

Data confidentiality

A successful health and social care App must ensure data confidentiality. Any failure to do so may result in a data breach, resulting in potential claims by individuals affected as well as an investigation and potential fine from the ICO or other regulators. That is without taking account of the reputational damage, which would likely reduce consumer confidence in the product and company which will consequently impact on revenue and the ability to enter the supply chain (particularly with large organisations such as the NHS).

Use of personal data should always be minimised (e.g. limited to data needed to achieve the intended purpose) and anonymised data should be used where possible. However, use of personal data is likely necessary for health care Apps. A potential solution to address the risk of being victim to a cyberattack and potential data breach is to apply cryptographic algorithms to encrypt data. Cryptographic algorithms are used for tasks including data encryption and authentication. The benefit to using cryptographic algorithms being that if exchanged data is intercepted, the attacker is not able to understand the content, so the risk is reduced.

When designing an App, you should ensure that the confidentiality of any personal data is properly managed by applying the following measures and ensuring these are reviewed and managed whilst the App is in use:

- data minimisation (e.g. only collect data which is necessary for the purpose) and review the amount of data collected periodically;
- data utilisation (e.g. using the data only in accordance with the purposes for which it was collected and in accordance with appropriate privacy policies);
- encryption (e.g. the process which renders data unreadable);

- managing data access and revocation (e.g. controlling access and limiting access to those on a strict ‘need to know’ basis, with users being required to have strong passwords and two-factor authentication where possible);
- managing physical security of devices and physical and electronic documentation as well as general computer use management (e.g. use of anti-virus software, routine patching, password protected devices and application access by users, suspension of session inactivity and enabling firewall);
- ensuring appropriate destruction (and deletion from electronic devices and cloud services or similar) of data once the purposes for which it was provided has expired or is no longer reasonable.

If engaging third party software developers, you should ensure robust obligations of confidentiality are also put in place, including, for example, the purposes for which information can be used and its restrictions on use.

The benefit of having such obligations in place is that if data is shared, either purposefully or accidentally, during App design and development, the risk that there is misuse of the data (which offers a commercial advantage rather than a bad faith use of personal data) can be addressed by having an enforceable right against that third party to (i) seek an injunction preventing further use; and (ii) claim damages for breach of contract. To the extent any registrable intellectual property right subsists in the App (which is prevented due to prior disclosure), you may have a remedy to pursue such registration if it can be established that the disclosure was made in breach of confidence.

Conclusion

Apps have a valuable place in the healthcare market and will likely continue to attract significant investment to produce better ways of delivering healthcare solutions. However, failing to address the above risks prior to starting App development has the potential to thwart any project timelines for implementation and commercialisation, but is also at increased risk of being subject to a future dispute and potential breach of an individual’s data rights.

Contact

Richard Nicholas

Partner

richard.nicholas@brownejacobson.com

+44 (0)121 237 3992

Related expertise

Health and life sciences