HERBERT SMITH FREEHILLS

DIGIHEALTH AND THE RACE FOR HEALTH DATA – KEY LEGAL ISSUES

The healthcare and pharmaceutical sectors in Asia and beyond are being reshaped by new digital technologies. From the use of AI for identifying lead compounds and connected devices for collecting personal health data, to the use of blockchain for managing supply chains and telehealth for accessing healthcare services, there are many exciting growth areas. These growth areas are driving a flurry of corporate deals, commercial collaborations and disputes. Meanwhile, healthcare regulators are being challenged to keep up to speed.

As big pharma meets big tech, health data (and access to it) is becoming "the new oil". It is vital for lawyers practising in this area to understand the nature of data, and how its collection and use may be impacted by data privacy, data security, and sector-specific regulations. This article examines some of the legal issues to consider in relation to digihealth collaborations, and in particular the use of health data.

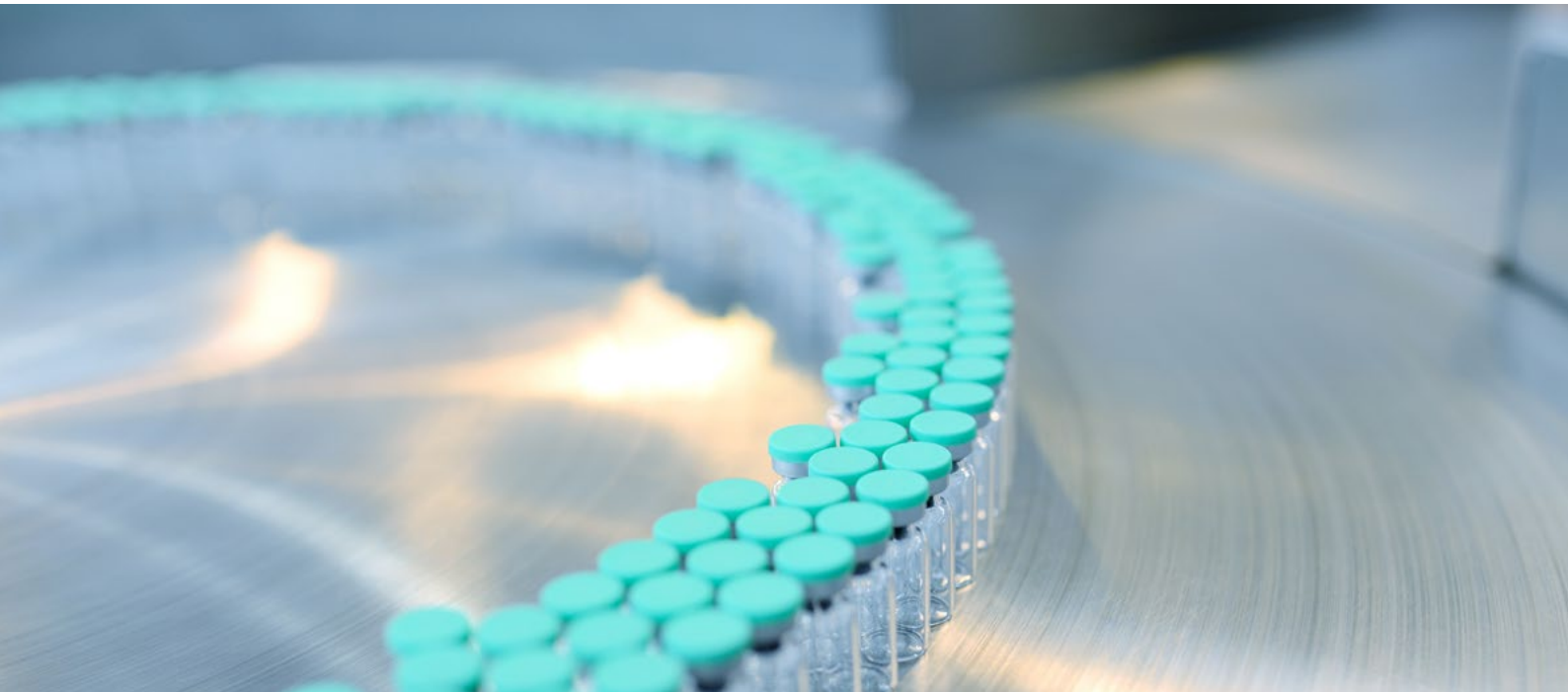
1. The changing landscape

Digital healthcare technologies have been on the rise in Asia (and beyond) for a number years. Concerned by aging populations and growing middle classes, governments across the region see digital healthcare technologies as potential solutions for: (i) providing all citizens with access to good-quality healthcare; (ii) preventing diseases and providing real cures (as opposed to the long-term management of chronic diseases); and (iii) reducing public healthcare spend. The global COVID-19 pandemic is giving new urgency to this "technolution", with both governments and corporates re-examining their digital health strategies.

Many of these technologies are being driven by the collection and analysis of vast and structured data reservoirs, which can be used to:

- expedite drug discovery;
- develop precision or personalised medicines;
- improve the efficacy and safety of medicines;
- improve patient compliance programs; and
- study and assess public health trends and projections, thus informing public and private health strategies, to both long term and short term challenges, including for example COVID-19 responses.

In this context, big pharma, device manufacturers, and traditional healthcare providers are turning to big tech for assistance.



2. Commercial collaborations

Traditional collaborations within the pharmaceutical and healthcare sectors usually focus on the development and commercialisation of pharmaceutical and medical device products. The path to success is long, complex, uncertain and very expensive, with many drug development programs running for upwards of 15 years and costing over US$2 billion. Importantly, the structure of these arrangements, and the roles and responsibilities of the parties (from research organisations and biotechs to big pharma and manufacturers), are relatively well defined. In contrast, the structure of digihealth collaborations, and the roles and responsibilities of the parties in such collaborations, can be less clear. This is because:

- **culture:** many tech companies involved in digihealth collaborations operate nimble, flexible and fast-moving businesses. They are often not used to dealing with the long-term and highly regulated nature of the pharmaceutical and healthcare sectors;
- **goals:** traditional collaborations typically start out by focussing on the development of a drug or device for the treatment of a particular disease or class of diseases, and have clear end-goals. It is not always so simple in the context of digihealth collaborations, which often have higher-lever objectives, such as optimising or developing new processes for the development of drugs and devices, or the provision of healthcare services, at the meta-level; and
- **profit and ownership:** with the convergence of players from different sectors, it can often be unclear how each party will monetise or own project outputs. For example, is each party free to exploit the project outputs within its own sector, or will the parties enter into a cross-licensing and profit sharing arrangement?

However, perhaps the biggest issue faced by our clients in this space relates to the collection, use and ownership of the health data that lies at the heart of many digital technologies.

3. Data

3.1 Health data

In its simplest form, data is simply information. However, when we talk about "health data" in the context of digihealth, we are really talking about data that relates to: (i) an individual who can be identified from that data, ie "personal data"; and (ii) the physical or mental health of the relevant individual (or their receipt of healthcare services), or the individual's genetic data, biometric data or behavioural patterns.

Health data may be collected from a range of sources, including genetic analysis, clinical trials, pharmacovigilance activities (ie monitoring of a drug's adverse effects), doctor and hospital patient records (including diagnostic and medical test records), other government databases, insurance databases, smart-devices, wearables and other connected devices, and even social media accounts. Once collected, health data can be stored digitally and organised into structured data reservoirs which may be processed and analysed, either alone or in combination with other data reservoirs, for various purposes.

3.2 Data as an asset

Although we often talk about data as an asset, the ownership and right to exploit data from a legal perspective can be difficult to define. This is because data are simply pieces of information and there is no general legal right to own and protect "information" per se. However, as organisations invest more time and money in collecting data, and large structured data reservoirs become more valuable, traditional notions around the ownership of data are being challenged. In the context of digihealth collaborations, we are seeing clients rely on both existing and new legal structures to manage the ownership and exploitation of data.

Perhaps the most reliable way to manage data is through express and clear contractual rights, for example, as set out in collaboration agreements, although an obvious limitation of contractual rights is that ordinarily they will only apply between the parties to the relevant contract, and not to third parties. Another basis for protecting data is through the use of copyrights, which can be used to protect certain databases. Although copyright can be enforced by the owner against the world at large, it can be difficult to establish that it both subsists within a relevant database, and has been infringed. In some circumstances, a party may rely on *sui generis* (ie specific statutory) forms of protection, such as database rights regimes (which will usually protect databases but not specific data) and trade secret regimes (which will not usually protect information that has been made public). Interestingly, some jurisdictions take a different approach. By way of example, a draft privacy bill in Indonesia suggests that personal data is owned by the relevant data subjects, and seeks to restrict the sale, purchase or monetisation of such personal data.

As can be seen, existing legal rights for the protection of data have limitations. These limitations are often put under pressure in the context of digihealth collaborations, and understanding their nuances is vital.

3.3 Data privacy

In addition to managing the ownership and commercialisation of health data from a commercial perspective, it is vital for parties to understand and comply with the regulatory requirements that may apply to the use of health data. Organisations that fail to comply with these measures can face serious fines and other sanctions, not to mention reputational damage.

One the challenges of operating within Asia is that each country within Asia has its own data privacy requirements. Furthermore, many digihealth collaborations involve parties based in Europe, the US, Australia and beyond, and often the data regulations of these jurisdictions can have an extra-territorial impact on collaborations based in Asia.

It is beyond the scope of this article to consider all of the data regulations across Asia (or beyond), but needless to say many jurisdictions follow (or are planning to follow), the principles set out in the GDPR, which is often seen as best practice when it comes to data privacy regulation. The GDPR places higher standards of protection on the use of health data than those in many jurisdictions in Asia.

Under Article 9 of the GDPR, the processing of health data is prohibited unless special exceptions apply, such as: (i) the provision of an individual's explicit consent; (ii) where processing is necessary for achieving purposes in the public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; (iii) processing is necessary for the purposes of "preventive or occupational medicine..., medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services" – provided that the health data is being processed by or under the responsibility of a "professional" who is under an obligation of professional secrecy; or (iv) scientific research purposes. Parties need to carefully consider whether these exceptions apply to particular digihealth arrangements.

In addition to the processing restrictions, the GDPR and similar personal data regulations around the world typically place limitations and restrictions on: (i) the transfer of personal data (including health data) across national borders (or the EU border); and (ii) the appointment of third party sub-processors. These restrictions can impact the use of health data in the context of digihealth collaborations, and the development of digital technologies, which involve the transfer of data: (i) out of country or (ii) to third party processors. Importantly, some countries within Asia, such as Indonesia, Vietnam, India and Pakistan, go further than the GDPR by requiring that certain classes of personal data, including "sensitive data" or "critical personal data" be "localised" and stored on-shore. In other words, it must not be transferred off-shore.

3.4 Data security

Data privacy regulations typically require data controllers to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of unauthorised use or disclosure of their data. Data controllers are also usually required to ensure that that each entity that access or processes data on its behalf has in place adequate security measures, and that it has adequate rights to verify such security measures (for example, audit rights and rights to be notified of security breaches). These security arrangements are of fundamental importance, not only from purely a regulatory perspective, but also a commercial, reputational and even ethical perspective.

Particular issues can arise in relation to complex digihealth collaborations where multiple parties are unclear on the precise storage, flow and use of health data, and the responsibilities of each party in relation to protecting the security of such data.

By way of a cautionary and high-profile example, in 2018 a cyberattack on SingHealth here in Singapore compromised the personal information of 1.5 million patients, including the prime minister Lee Hsien Loong. In this case, SingHealth had delegated responsibility for maintaining its IT security to IHiS, which failed to take adequate measures to protect personal data in its possession. In issuing record fines of SGD750,000 to IHiS and SGD250,000 to SingHealth, the Singaporean PDPC said, "even if organisations delegate work to vendors, organisations as data controllers must ultimately take responsibility for the personal data that they have collected from their customers".

There are numerous other examples of cyber attacks on health data, with some reports suggesting that healthcare is now the most targeted sector by hackers (ahead of banking, insurance and financial sectors).

Importantly, beyond pure data breaches, cyber risks for the sector can damage valuable information assets and systems, and disrupt research and development operations, distribution and care delivery across entire supply chains.

3.5 National regulations and beyond

Numerous countries across Asia and beyond are imposing more specific healthcare/healthtech-specific regulations that have the potential to impact the use of health data. More general laws also have the potential to impact digihealth collaborations, such as antitrust laws which may prevent the monopolisation of vast health data reservoirs. Such regulations will continue to evolve in order to keep pace with emerging digihealth technologies, and will need to be considered on a case-by-case and country-by-country basis for digihealth collaborations.

Beyond strict legal requirements, there is a growing global movement that is focussing on data ethics and data governance, both within the pharmaceutical and healthcare sectors and beyond. This movement is giving rise to interesting questions about the collection and use of big data, data sovereignty, the value of data and the rights of data subjects to be remunerated for the exploitation of their personal health data, and the role to be played by nation states, state bodies, private companies and other organisations. The movement is also increasingly being taken into consideration by regulators.

4. Conclusion

Driven by government policy and the collection and analysis of vast and structured data reservoirs, the rapid growth and adoption of digital healthcare technologies looks set to continue for the foreseeable future. As it does, research organisations, biotechs, big pharma and healthcare providers will need to navigate new commercial and regulatory challenges in order to take full advantage of the new technologies. This will require a nuanced understanding of health data, and the rules governing its collection, ownership and use. At the same time, organisations will need to consider broader ethical and data governance issues in order to ensure they maintain strong relationships with their patients, communities and regulators.

Key contacts

Natalie Bryce
Partner
Brisbane
T +61 7 3258 6574
natalie.bryce@hsf.com

Rebekah Gay
Partner
Sydney
T +61 2 9225 5242
rebekah.gay@hsf.com

Gavin Guo (HSF/Kewei)
International Partner
Mainland China
T +86 21 2322 2171
gavin.guo@hsfkewei.com

Harry Evans
Senior Associate
Singapore
T +65 6868 8079
harry.evans@hsf.com

Vik Tang (HSF/HBT)
Partner
Jakarta
T +62 21 3973 6118
vik.tang@hsf.com

Christopher Hunt
Partner
Tokyo
T +81 3 5412 5401
christopher.hunt@hsf.com

Cellia Cognard (HSF/HBT)
International Counsel
Jakarta
T +62 21 3973 6125
cellia.cognard@hsf.com

For a full list of our global offices visit **HERBERTSMITHFREEHILLS.COM**