VIEWS AND OPINIONS

LEGAL PERSPECTIVE

[datalex]

BALANCING THE LEGAL, ETHICAL, AND PRACTICAL ASPECTS OF USING DIGITAL HEALTH TECHNOLOGIES IN CLINICAL RESEARCH

Author: **Gabriel Avigdor**

Affiliations: Attorney-at-law; datalex LLC, founder; Certified Information Privacy Professional/Europe (CIPP/E); Bar Association of the Canton of Vaud (OAV), member; Swiss Bar Association (SAV), member; University of Geneva, Faculty of Medicine, MAS/DAS lecturer; and Haute Ecole Arc (HE-Arc), lecturer

doi: 10.54920/SCTO.2024.RAWATCH.9.25

Digital health technologies bring innovation to participants in clinical trials. They enable the collection, use, and sharing of large amounts of data for medical and scientific research purposes, which ultimately benefits patients. In the context of drug development, traditional clinical trials face significant privacy challenges due to a lack of harmonisation and diverging interpretations of privacy laws and authorities' guidance. Given the use of digital health technologies, decentralised trials in particular have to manage an additional level of complexity. Involving technology providers increases concerns around the access, storage, and security of study data. Authorities, ethics committees, and healthcare institutions often ask for various additional or bespoke requirements that may diverge from or even conflict with each other, which can lead to unintended consequences for research initiatives and for individuals who are willing to participate in innovative clinical trials. This article outlines some legal, ethical, and practical issues as well as their consequences when using digital health technologies in the research sector.

The COVID-19 pandemic motivated public and private stakeholders to make significant and fundamental changes to conservative practices in the healthcare sector, for example by allowing and adopting digital health technologies (**DHTs**). Within only a few months, authorities, academics, institutions, healthcare providers (**HCPs**), private actors, and people around the world had to start using technologies that, without the sense of urgency caused by the pandemic, would have taken decades to accept, adopt, and implement in the healthcare landscape.

In the context of clinical trials, health authorities granted approvals or concessions that were limited in time and allowed remote care, patient monitoring, and accelerated procedures in order to develop a COVID-19 vaccine. The adoption of such technologies set a standard and an expectation in the healthcare and clinical research sectors that remained after the pandemic, and it accelerated digital initiatives such as remote meetings, online medical screening tests, and decentralised clinical trials (**DCTs**). However, while the use of advanced technologies has increased since the pandemic and has led to significant progress in many sectors, the use of DHTs within clinical research activities has not kept pace with those developments.

FROM PRIVACY BENEFITS TO LEGAL ISSUES

DCTs aim for a decentralised study set-up, which means moving away from using only the infrastructure of the study site (centralised model) to having participants become the point of care, for example in their homes. Participants can take part in a study while interacting remotely with the study team, they can access additional medical materials through web applications, and it is possible to avoid travelling to or staying in the hospital. DCTs also have the potential to implement customised data privacy measures, a benefit that gives participants more control over their data and better security by using unique and controlled devices, applications, and processes specifically designed for and provided by the study.

Although not all participants may fully understand or appreciate how innovative web platforms and mobile application work in detail, the use of DHTs in clinical research still remains compatible with bioethical principles because they enable broader access (beneficence) for a more diverse part of the population (justice) to clinical trials and novel treatments.[1,2] As DHTs raise many other legal and ethical issues that cannot be covered in detail within this article, the focus will mainly be on the tensions between participants' fundamental rights to privacy and their access to innovative research initiatives.

Data privacy and data protection in the healthcare sector is a heavily debated topic, and the nuances and technical aspects are largely misunderstood by non-privacy professionals. Because DCTs combine technical, legal, and technology aspects in a heavily regulated environment that allows countries to provide their own legislation, national authorities have brought diverging interpretations and guidance on privacy and security requirements. Often, this forces sponsors to comply with practices that are not harmonised within the same study (e.g. multinational studies). The spirit of most emerging, comprehensive privacy laws focuses on clear goals: implementing privacy and security standards, increasing accountability and transparency, and enabling the enforcement of privacy rights while limiting the ability of big tech companies to conduct disproportionate data processing activities. Under the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use Guideline for Good Clinical Practice (**ICH GCP**), there is no specific reference to data protection laws. Therefore, the relevant national or regional legislation applies. New privacy laws, such as the EU's General Data Protection Regulation (**GDPR**), have produced immediate and noticeably positive effects: a huge increase in the number of full-time privacy professionals, a higher level of knowledge and awareness among the general public, stricter obligations for organisations handling personal data for defined purposes (data controllers), robust privacy compliance programmes, and enforcement actions by authorities, especially in Europe.

Unfortunately, there are downsides to the increase in data protection, especially because everyone wants to have a say – including privacy experts and non-experts. As a result, fundamental privacy concepts and principles, which should remain the same everywhere, are not interpreted in the same way across regions, in different countries, and sometimes even within the same country. This creates legal uncertainty, a lack of harmonisation, delays in approving study protocols, and tough discussions in contract negotiations. Major differences exist in the following areas:

- **Roles of the parties:** Determining and allocating the roles of the parties as either data controller, data processor, or joint controller is still fundamentally different.
- **Choosing the appropriate legal basis:** Using consent or another legal basis for the use of personal data for primary research or further research differs drastically between countries, authorities, and research projects.
- **Informed consent forms:** The content and length of informed consent forms vary.

It is hard to justify to individuals willing to participate in the same trial how there can be many differences between one country and another, especially when such differences do not provide any additional privacy protections to their personal data. Instead, these differences create inconsistencies and make it more difficult to run multinational studies, in particular when new technologies are used. Privacy laws provide strict transparency requirements for participants and strong accountability obligations for data controllers handling participants' sensitive personal data. From an ethical point of view, all participants should be treated equally – even though this is not mentioned in privacy laws. Yet given these divergences, participants are not treated equally with regard to data protection.

Below are some more ethical, legal, and practical issues that are relevant when using DHTs in innovative trials but that can also become obstacles for research initiatives, thus hindering individuals' access to those trials.

DATA TRANSFERS

When conducting DCTs, sponsors need to work with specialised technology providers to facilitate the creation of a secure online infrastructure. Inevitably, data (including study participants' sensitive personal data) will have to flow between countries and will be accessible by multiple stakeholders who need to maintain the confidentiality, integrity, availability (**CIA**), and security of study data at all times. This originates not only from privacy laws but also from international standards such as the ICH GCP. The transfer of personal data to other countries has sparked animated discussions and debates. Indeed, after the uncovering of the Edward Snowden scandal on 5 June 2013[3] and the Schrems II decision from the Court of Justice of the European Union (**CJUE**) in July 2020 invalidating data transfers from Europe and Switzerland to the United States,[4] data transfer is still being hotly debated.

In reality, the risk that foreign authorities can request access to participants' personal data is extremely small. Moreover, they most likely have no interest in this data. Study participants' data is key-coded and thus particularly protected against re-identification, which is quite unique compared to other industries. Therefore, the debate around cross-border data transfers remains rather theoretical. Experience has shown that concerns about participants' information and sensitive data becoming accessible and thus being used by third parties outside of the research environment stems from fears of losing control, even though the use of a third-party secured solution is often inevitable and more secure when using new technologies and online platforms. Therefore, the focus on restricting cross-border data flow can be seen as pointless. In fact, companies and organisations conducting research globally already use IT systems running on secure, state-of-the-art, third-party infrastructures – even if they do not use DHTs.

DATA LOCALISATION

Using third-party IT systems usually involves cloud-based environments with foreign data centres belonging to big tech companies, such as Amazon Web Services or Microsoft Azure. These hosting providers have among the strongest and most reliable security infrastructures in the world, as opposed to local storage infrastructures at healthcare organisations. Even so, data localisation often creates emotional and animated discussions. Researchers are rightly concerned whenever participants' data leave their premises since they must preserve medical secrecy and prevent access to medical records by unauthorised individuals and organisations. Furthermore, authorities and ethics committees act as the ultimate guarantor of participants' interests.

Strict data localisation requirements, however, are often incompatible with cross-border data sharing and clinical research initiatives. In fact, most privacy laws around the world, including Switzerland's Data Protection Act (**FADP**), do not require any data localisation. A very limited number of countries close their digital borders in order to have political control over information in their territory, for example China,[5,A] France to a certain degree for the hosting of medical health data,[6,B] and Russia.[7,C] In general, privacy laws already strictly regulate the transfer of personal data to foreign countries that have no equivalent data protection legislation, and they require contractual, legal, and technical guarantees (i.e. appropriate safeguards and transfer impact assessments). As a result, data localisation requirements are not legally needed, and battling for data localisation or transfer restrictions does not add more protection for participants' personal data. Instead, it encourages country shopping (i.e. selecting countries that are more permissive) and decreases the chances of researchers sharing data across countries.

ELECTRONIC SIGNATURES AND CONSENT

Switzerland is one of the only countries to require a qualified signature (the digital equivalent of a handwritten or "wet" signature) to electronically sign documents.[D] However, using a qualified signature is a costly process in which the validation of a signature requires submitting a request and evidence to a trusted third party.[8–10, E] Requiring participants to use a qualified signature to sign their informed consent form electronically has proven unfeasible in practice. Instead, participants have been required to sign, scan, and send the document by email or post – or to travel to study site and deliver it personally. As a result, Switzerland has struggled to adapt to the digital age and favour innovation. The good news is that the since the revisions to the Clinical Trials Ordinance (**ClinO**) came into effect on 1 November 2024, the newly introduced Article 7c now permits using electronic means to obtain individuals' consent to participate in a clinical trial, provided that the authentication mechanism uses "a method which unequivocally identifies the person concerned". This marks a significant advancement, allowing the use of digital means of identification without requiring the strictest method of authentication.

TO IDENTIFY, OR NOT TO IDENTIFY, THAT IS THE QUESTION!

On the one hand, sponsors have to ensure they cannot access a participant's identifiers. And on the other hand, they must also be able to verify a participant's identity, for example when using an online platform, which is a challenging task. In addition, study participants' personal data must remain in a key-coded format (using a unique identifier or number for each participant),[F] and neither sponsors nor third-party providers should

[A] The Cyberspace Administration of China (**CAC**) reviews and approves transfers of personal data outside of mainland China. China had strict data localisation requirements, which have now been loosened. See Luo and Dan's 2024 blog post "China Eases Restrictions on Cross-Border Data Flows".
[B] The French data protection authority CNIL has introduced a unique privacy scheme requiring compliance with MR methodologies (*méthodologies de référence*), which require submission or prior authorisation for any major deviations. In addition, France has introduced data localisation requirements by updating its public health code under article L.1111-8 for hosting health data to cloud providers outside of clinical trials.
[C] In September 2015, Russia made it mandatory to localise databases containing the personal data of Russian citizens in the Russian territory. In addition, personal data transfers require prior notification to Russia's data protection authority (Roskomnadzor).
[D] See Articles 12–14 of Switzerland's Federal Code of Obligations, Article 2, letter e of the Federal Act on Electronic Signatures, and Article 16, paragraph 1 of the Human Research Act.
[E] In Europe, the Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (**eIDAS**) defines levels of signatures, including an advanced signature that provides less costly options. For more information, see the European Commission's "eSignature FAQ" web page.
[F] Pseudonymised data as defined by Article 4 of the General Data Protection Regulation (**GDPR**) is still considered personal data and is not considered anonymised.

be able to re-identify participants.[11,G] If a component used in a DCT involves a web portal, the simple fact that a participant logs into an online platform requires an authentication mechanism, which can include a full name, an email address, a password, and sometimes a phone number for two-factor authentication purposes. The collection of a participant's personal data is therefore inevitable at the login stage, unless a randomly generated code is sent to an email address that does not contain the participant's name, which is complicated. In all cases, participant identification is necessary yet restricted under the ICH GCP.

Secondly, once a participant logs into a platform and is authenticated, the platform will have to track the participant's identity for security, traceability, and safety purposes, especially if the individual uses a web portal to sign an electronic informed consent form (**eICF**) agreeing to participate in a study, access specific medical information, plan online meetings, access study data, use an e-diary, or agree to have medical equipment shipped to his or her home. Managing and controlling how these platforms' technology providers and sponsors access participants' health data without having the right to identify them is a technical and legal catch-22 situation. Therefore, in order for it to be possible to conduct innovative trials such as DCTs more efficiently, authorities and ethics committees must admit and authorise the use of certain limited personal data for identification, authentication, and security purposes.

STUDY CONSENT AND PRIVACY CONSENT: A BIG MISUNDERSTANDING

Under most countries' data protection laws (including those in Switzerland, the UK, and the European Economic Area), the processing of sensitive health data does not always require obtaining consent. Data controllers often have a transparency obligation and can rely on a legal basis other than consent, such as using exemptions or derogations based on legitimate interest, private interest, vital interest, scientific research, fulfilment of a contract, or a legal obligation (e.g. to monitor patient safety and adverse events). An informed consent form (**ICF**) typically includes a detailed, bespoke, clear, concise, and unambiguous text in the form of a privacy notice or privacy statement section to explain what data will be collected, why it will be collected, and how and by whom it will be used for the purpose of the study.[H]

However, some authorities and national guidance still request two different types of consent: the first is consent to participate in a trial (i.e. allowing an individual to decide whether or not to participate), and the second is consent for the processing of personal data. Informed consent is the expression of a free choice and remains valid only if sufficient information is provided and consent is freely given. When an individual decides to participate in a clinical trial, obtaining consent to participate is mandatory. In clinical research, though, asking for the second type of consent for using sensitive personal data does not constitute a free choice. Since a participant's data are necessary for a study, an individual cannot freely decide to participate in a study while simultaneously refusing to share his or her personal data. This contradiction should be self-evident. In practice, though, requests for consent to process personal data are often treated independently of the choice to participate in a clinical trial. And yet if an individual does not consent to share their personal data for a study, they cannot participate in the study. This means that when an ICF contains a specific and separate consent for the use of personal data for the study, consent cannot be freely given because participation is contingent upon it. As a result, such consent becomes invalid, rendering the processing of personal data unlawful.

Well-drafted privacy notices should provide enough information and transparency to enable participants to make an informed decision while ensuring that competent bodies and institutions have the assurance that study data will remain secure, available, traceable, confidential, and of good quality for research purposes. When appropriate and relevant, an ICF should also outline in broad terms which technology is optional or mandatory for participants, who will access participants' personal data, and for what purposes their data will be accessed.

With all the debates around privacy, it is easy to forget that the main goal of a study is to improve participants' health through new treatments. Individuals will likely prioritise understanding the potential adverse effects of an investigational medicinal product when deciding whether or not to participate in a clinical trial. Therefore, while privacy remains an important fundamental human right that requires due care, it is essential not to lose sight of the fact that individuals with a serious illness or condition most likely focus more on improving their health and accessing new medicines or novel treatments than on concerns about documents and data they consent to share.

[G] See sections 1.58 (subject identification code) and 5.17.1 (adverse drug reaction reporting) of the European Medicines Agency's Guideline for Good Clinical Practice E6(R2).
[H] See, for example, Article 12 of the EU's GDPR and Article 19 of Switzerland's FADP.

CONCLUSION

The emergence of modern data protection legislation – such as the EU's GDPR and Switzerland's FADP – has led to positive outcomes that have improved the respect of privacy as a fundamental human right and the protection of trial participants' sensitive personal data. This is especially relevant as digital health technologies are increasingly being used in clinical trials. Position papers, recommendations, and guidance developed by authorities are legally non-binding. However, in practice they are closely monitored and analysed by clinical research sponsors and technology providers. Given their inconsistencies and sometimes excessive requirements, research initiators may choose to conduct their trials in more permissive countries with less burdensome administrative and legal conditions – potentially to the detriment of trial participants. Most privacy-related debates in clinical research do not focus on what can be considered important for the participant's ultimate benefit. The creation of detailed, specific, and local deviations or requirements in Europe and among authorities (including in Switzerland) has generated an ecosystem of divergences and restrictions and led to disharmonised practices that are extremely difficult to navigate when considering starting a multinational clinical trial.

Decentralised clinical trials offer many promising benefits. However, they are conducted within a political landscape where countries and authorities view strict consent requirements (as a wrong sense of choice), data localisation, and transfer restrictions as the solution to competitiveness. Unfortunately, the significant divergences in legislation and guidance, the lack of harmonisation in practices, and obstacles for initiating trials with decentralised components all affect innovation and hinder some participants from benefiting from scientific research globally. The result is a paradoxical situation in which placing too much emphasis on the protection of participants' data (resulting in excessive measures) can undermine research initiatives that predominantly aim to improve people's health and well-being. It also results in study participants in the same study being treating differently in different countries or regions, which can be considered unethical. Privacy protection and the security of participants' data is paramount. However, the importance of privacy and its weight in discussions and negotiations to initiate trials have direct consequences for individuals willing to participate in trials. Data protection remains a fascinating, crucial, and technical area that continues to evolve over time. Driving innovation by implementing new technologies in clinical trials initiatives presents legal, ethical, and practical challenges. In order to facilitate scientific research initiatives using new technologies and favour innovation for the ultimate benefit of participants, authorities and all stakeholders involved in clinical studies should strive to develop harmonised practices and common guidelines that promote and accelerate research instead of introducing overly strict regulations, requirements, and restrictions.

REFERENCES

[1] US Department of Health, Education, and Welfare (1979) The Belmont Report. Accessed 2 December 2024: https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf

[2] Lawrence DJ (2007) The four principles of biomedical ethics: A foundation for current bioethical debate. Journal of Chiropractic Humanities 14:34–40. doi: 10.1016/S1556-3499(13)60161-8

[3] Greenwald G (2013 June 6) NSA collecting phone records of millions of Verizon customers daily. The Guardian. Accessed 28 October 2024: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[4] Mildebrath H (2020) The CJEU judgment in the *Schrems II* case. European Parliamentary Research Service. Accessed 28 October 2024: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

[5] Luo Y and Xuezi D (2024 Mar 25) China eases restrictions on cross-border data flows. Covington [blog]. Accessed 28 October: https://www.insideprivacy.com/uncategorized/china-eases-restrictions-on-cross-border-data-flows/

[6] Commission Nationale de l'Informatique et des Libertés (2021) Recommandations provisoires: Contrôle qualité à distance des essais cliniques pendant la crise sanitaire liée à la COVID-19. Accessed 28 October 2024: https://www.cnil.fr/sites/cnil/files/atoms/files/recommandations_provisoires_-_controle_qualite_a_distance_des_essais_cliniques_pendant_la_crise_sanitaire_liee_a_la_covid-19.pdf [in French]

[7] Blinov O (2020 Dec 17) Encrypt your data to make GDPR and Russian data localization law compatible. IAPP. Accessed 28 October 2024: https://iapp.org/news/a/encrypt-your-data-in-order-to-make-gdpr-and-russian-data-localization-law-compatible

[8] European Commission (n.d.) eSignature FAQ. Accessed 28 October 2024: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature+FAQ

[9] swissethics (2024) Guidance document on the development and use of an electronic informed consent (eIC) (version 2.1, dated 25 August 2024). Accessed 28 October 2024: https://swissethics.ch/assets/studieninformationen/240825_guidance_e_consent_v2.1_web.pdf

[10] Swissmedic and swissethics (2022) Position paper on decentralised clinical trials (DCTs) with medicinal products in Switzerland (version 2.0, dated 15 December 2022). Accessed 28 October 2024: https://www.swissmedic.ch/dam/swissmedic/en/dokumente/bewilligungen/klv/positionspapier-dct.pdf.download.pdf/DCT_EN_.pdf

[11] European Medicines Agency (2018) Guideline for good clinical practice E6(R2) (version dated 1 December 2016). Accessed 28 October 2024: https://www.ema.europa.eu/en/documents/scientific-guideline/ich-guideline-good-clinical-practice-e6r2-step-5_en.pdf