3

Challenges of Remote Patient Care Technologies under the General Data Protection Regulation

Preliminary Results of the TeNDER Project

Danaja Fabcic Povse

I INTRODUCTION

Patients with complex diseases like Alzheimer's or Parkinson's often require round-the-clock care. Since caregivers may not always be able to be present, remote care technologies (RCTs) can supplement human caregiver intervention and provide the patient with better care. In the TeNDER project,[1] we are building technology that will create an alert system for caregivers: For example, if the person falls, their relative or nurse receives a phone alert and can go and check up on them. Such technology relies on remote patient monitoring to detect anomalies in the person's environment and combines data sources, including electronic health records (EHRs) and data from connected devices (e.g., wearables). The use of these technologies raises questions of data protection since especially sensitive data are involved.[2]

Legal frameworks that govern the use of RCTs are, by their nature, abstract and high-level, meaning that their application might not take into account the specific type of technology or its use in a particular care situation, leaving developers and users in an unclear legal situation.[3]

This chapter aims to bridge the gap between the high-level data protection framework and practical, micro-level application of RCTs by providing an overview of the challenges under European Union (EU) law when developing and using RCTs, exploring how initial results from the TeNDER project on resolving those challenges can help with the practical implementation of similar solutions, as well as examining gaps in the regulation itself. Using these technologies as a starting point, the chapter analyzes the obligations the General Data Protection Regulation

[1] See generally TeNDER Health – TeNDER Project, www.tender-health.eu/. Disclaimer: This research has been funded by the European Commission under the Horizon 2020 mechanism – grant no. 875325 (TeNDER, affecTive basEd iNtegrateD carE for betteR Quality of Life).

[2] Eur. Parliamentary Rsch. Serv., *The Rise of Digital Health Technologies During the Pandemic* (2021), www.europarl.europa.eu/RegData/etudes/BRIE/2021/690548/EPRS_BRI(2021)690548_EN.pdf.

[3] Craig E. Kuziemsky et al., Ethics in Telehealth: Comparison between Guidelines and Practice-based Experience – The Case for Learning Health Systems, 29 Y.B. Med. Informatics 44 (2020).

https://doi.org/10.1017/9781009373234.005 Published online by Cambridge University Press

(GDPR) lays upon developers in order to address the following research question: "What challenges does the GDPR pose for designers of remote patient care technologies (RCTs), and how can those questions be addressed in practice?"

To answer the research question, the chapter first introduces key legal concerns that data protection poses regarding the use of RCTs, focusing on their field of application and the key principles and obligations relevant to developers. At the same time, the work draws upon the preliminary results of the TeNDER project (2019–2023) to discuss any potential shortcomings in the regulation.

The RCTs discussed in this chapter are in-house, as they are specifically developed to be used remotely, and digital, including digital technologies such as wearables, smart devices, microphones etc. However, TeNDER is not designed to be a medical device and, thus, performs no diagnostics.

II REMOTE CARE TECHNOLOGIES AND THE GDPR

RCTs are a type of technology that can help patients manage their illnesses better, as well as help elderly people live more independently. They can be used institutionally (e.g., in a care home or hospital) or in the home, where they can contribute to a better quality of life for the user. A variety of different technologies can be used – monitoring devices, smartphones, apps, social media, videoconferencing tools, etc.[4] RCT is distinct from telehealth or eHealth, which refer to the phenomenon of digital health care in general, while remote monitoring or remote care describes the technology (or technologies) being used. RCT is, thus, a specific technology that is used by health care providers, either in a telehealth or a classical health care setting.[5]

The advent of 5G and the Internet of things, combined with the two years of pandemic, has led to a heightened uptake of telehealth solutions, including remote monitoring applications and wearables that help people age better.[6] The use of RCTs is especially beneficial for older adults with chronic conditions, for whom monitoring devices, communication tools, and follow-up phone calls enable the 24-hour availability of health management tools.[7]

RCTs, like many other eHealth technologies, rely on advanced data processing techniques and different devices, both medical and general-purpose ones, to provide functionalities. The devices and technologies must, at the same time, meet the goals they were designed for and ensure patients' privacy and safety.[8] In terms

[4] Alexandra Queirós et al., Remote Care Technology: A Systematic Review of Reviews and Meta-Analyses, 6 *Technologies* 22 (2018).

[5] Caregility Team, *The Difference Between Remote Patient Monitoring and Telehealth*, https://caregility.com/blog/the-difference-between-remote-patient-monitoring-and-telehealth/.

[6] Eur. Parliamentary Rsch. Serv., supra note 2.

[7] Queirós et al., supra note 4.

[8] Ana Isabel Martins et al., Ambient Assisted Living: Introduction and Overview, in *Usability, Accessibility and Ambient Assisted Living* 1 (Alexandra Queirós & Nelson Pacheco da Rocha eds., 2018).

https://doi.org/10.1017/9781009373234.005 Published online by Cambridge University Press

of data privacy, patients risk losing control over their health data – especially when it comes to their EHRs[9] – when remote monitoring devices, such as wearables, are used.[10] Elderly users may not have consented to the processing of their health data; they may consider monitoring devices as a form of spying upon their private lives.[11]

The GDPR,[12] adopted in 2016, binds controllers and processors involved in the processing of health data to put in place appropriate technical and organizational mechanisms to ensure patients' data protection and the confidentiality of medical information.

The first issue is determining the GDPR's scope of application to RCTs. The regulation applies when personal data, defined as "any information relating to an identified or identifiable natural person ('data subject')" (art. 4(1) of the GDPR), are being processed, meaning "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring," and so on (art. 4(2) of the GDPR). Data concerning health (also referred to as health data) are defined as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status" (art. 4(15) of the GDPR).

How can we determine what constitutes personal data in a remote care scenario? As per the definition of art. 4(1), as long as information can be linked to a data subject, it is considered personal data. Since the scenario deals with a health care setting, health data are very likely going to be processed. More specifically, the 2007 opinion of the Article 29 Working Party states that "all data contained in medical documentation, in electronic health records and in EHR systems should be considered to be 'sensitive personal data.'"[13] However, data that cannot be linked to a data subject is not considered personal data, for example because it has been irreversibly anonymized.[14]

The regime under the GDPR is centered on a data controller, a central entity in charge of the processing activity, which determines the purposes and means of the processing (art. 4(7) of the GDPR). In order to process data, a controller must

[9] Benedict Stanberry, Telemedicine: Barriers and Opportunities in the 21st Century, 247 J. of Internal Med. 615 (2000).

[10] I. Glenn Cohen et al., Ethical and Legal Implications of Remote Monitoring of Medical Devices, 98 Milbank Q. 1257 (2020).

[11] S. Stowe & S. Harding, Telecare, Telehealth and Telemedicine, 1 Eur. Geriatric Med. 193 (2010).

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (GDPR) (text with EEA relevance), 2016 O.J. (L 119) 1, http://data.europa.eu/eli/reg/2016/679/oj/eng.

[13] Article 29 Working Party, Eur. Commn', *Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR)* (2007), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf.

[14] Article 29 Working Party, Eur. Commn', *Opinion 05/2014 on Anonymisation Techniques* (2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm.

comply with data quality principles, such as data minimization and accuracy (art. 5(3) and 5(4) of the GDPR, respectively), and ensure the existence of valid legal grounds, as per art. 6 of the GDPR. Controllers can engage processors to help them carry out the processing operation – art. 4(8) of the GDPR defines a processor as a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Since RCT relies on different technologies and different service providers, defining the controller and the processor may be difficult. Recent decisions of the Court of Justice of the EU, such as *Wirtschaftsakademie*[15] and *Fashion ID*,[16] as well as advisory opinions,[17] point to an "essential means" test. Essential means are key elements which are closely linked to the purpose and the scope of the data processing, such as whose data will be processed, which data types, for how long, and who will have access to them. The entity that determines the essential means of processing is, therefore, the data controller.

Determining the controller is important for ensuring that the right party can demonstrate compliance with the applicable principles and obligations ("accountability" – art. 5(2) of the GDPR). Among them are the data quality principles of art. 5(1): Lawfulness, fairness, and transparency; purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. The controller is further responsible for implementing appropriate technical and organizational measures ensuring compliant processing (art. 24(1) of the GDPR) and for building privacy into the system by design and by default (art. 25(1)–(2) of the GDPR). Moreover, proactively implementing data protection during the development process helps eventual adopters in ensuring compliance, especially with the data protection by design approach.[18]

III THE TENDER APPROACH

The TeNDER project, funded by the Horizon 2020 mechanism, seeks to empower patients with Alzheimer's, Parkinson's, and cardiovascular diseases, by helping them to monitor their health and manage their social environments, prescribed

[15] Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* v. *Wirtschaftsakademie Schleswig-Holstein GmbH*, interveners: Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht, ECLI:EU:C:2018:388 (June 5, 2018).

[16] Case C-40/17, *Fashion ID GmbH & Co. KG* v. *Verbraucherzentrale NRW eV*, interveners: Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, ECLI:EU:C:2019:629 (July 29, 2019).

[17] Eur. Data Prot. Bd., *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR* (2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en.

[18] Ann Cavoukian, International Council on Global Privacy and Security, By Design, 35 IEEE Potentials 43 (2016).

https://doi.org/10.1017/9781009373234.005 Published online by Cambridge University Press

treatments, and medical appointments. It follows an integrated care model, linking both medical and social aspects, such as (mis)communication and the fragmentation of care. The development process combines existing technologies, such as smartphones, wearables, and sensors, in order to monitor vital signals or alert a caregiver in case of an accident or fall, always consulting with patients to account for their preferences.[19]

As a research project, TeNDER crosses a number of different legal frameworks. Concerning the development process, we have focused on the requirements found in the GDPR, such as the legal basis for processing health data, privacy by design, and pseudonymization measures, and addressed the potential applicability of the Medical Devices Regulation. Once the results are finalized and marketed to health care organizations and caregivers, the preliminary legal findings, contained in several reports conducted through the lifecycle of the project, can serve as guidance to adopters.

In the project, we have adopted a three-step methodology to address the gaps in the regulation of eHealth technologies and to establish good practices for lawful and ethical implementation. First, a benchmark report identified applicable laws and ethical principles in abstracto and analyzed the initial concerns of the nexus between technology and applicable frameworks.[20] Building upon its findings, the three follow-up impact assessments take into consideration privacy, data protection, ethical-societal aspects, and the regulation of medical devices.[21] The final legal report, released in April 2023, provided an evaluation from legal and ethical perspectives of the technologies developed during the project, as well as recommendations for future adopters.[22]

Since the development of eHealth products necessarily takes place in a controlled environment, with a limited number of participants and the roles of different providers known in advance, the legal requirements in a post-project, real-life setting may vary slightly. For example, if the pilots in the project are based on small patient groups, a data protection impact assessment (DPIA) is not always necessary as per art. 35 of the GDPR, while in a larger organizational context it may well be obligatory.[23]

[19] TeNDER Health – How TeNDER Works, www.tender-health.eu/project/how-tender-works/.

[20] TeNDER, *D1.1 "First Version of Fundamental Rights, Ethical and Legal Implications and Assessment"* (2020), www.tender-health.eu/project/.here-you-can-find-a-selection-of-the-projects-public-deliverables-as-they-become-available/.

[21] TeNDER, *D1.4, "First version Legal/Ethical Monitoring and Review"* (2021), www.tender-health.eu/project/here-you-can-find-a-selection-of-the-projects-public-deliverables-as-they-become-available/.

[22] TeNDER, *D1.6, "Final Version of Fundamental Rights, Ethical and Legal Implications and Assessment"* (2023), www.tender-health.eu/project/here-you-can-find-a-selection-of-the-projects-public-deliverables-as-they-become-available/.

[23] Danaja Fabcic Povse, Fragmented eHealth Regulation in the EU TeNDER (2022), www.tender-health.eu/fragmented-ehealth-regulation-in-the-eu/.

IV ADDRESSING DATA PROTECTION CHALLENGES: LESSONS LEARNED IN TENDER

A *Roles and Obligations*

In a remote care scenario, the controller will be processing patients' health data, which are considered particularly sensitive due to the data's intimate character. Therefore, a stricter regime applies: Under art. 9, the processing of health data (and other special categories of data) is not permitted, unless one of the criteria in art. 9(2) is met. In this kind of scenario, that could be the explicit consent of the data subject unless prohibited under EU or national law (art. 9(2)(a)). Alternatively, the processing of health data is permitted if the processing is necessary for protecting the vital interests of the data subject, or another person when the data subject is incapable of giving consent (art. 9(2)(c)), such as when the patient is unconscious following an accident. Finally, processing is also permitted if the personal data have been made manifestly public by the data subject (art. 9(2)(d)), which happens when the data are already available to the caregiver or have been published on a social media platform.

In the TeNDER project, we identified legal grounds for consent from art. 6, with the explicit consent from art. 9(b) as an exemption from the art. 9(a) prohibition of processing. However, as many patients with Alzheimer's and Parkinson's diseases experience a decrease in cognitive function, ensuring the informed-ness of their consent can be a challenge. While the GDPR contains special rules for *children's consent* (art. 8 of the GDPR), there is no similar rule for obtaining informed consent from *incapable adults*, nor is this gap addressed in the relevant guidelines of the European Data Protection Board (EDPB).[24]

To resolve this legal gap and ensure that patients were fully briefed, they were provided with both lengthy and simplified information sheets, following bioethical recommendations contained in several (nonbinding) international documents, such as the Declaration of Helsinki and the Council of Europe Recommendation No. R(99)4 on Principles Concerning the Legal Protection of Incapable Adults.[25] While these are not requirements for consent under binding law, they contribute to better involvement of patients with Alzheimer's in research projects.[26]

[24] Eur. Data Protection Bd., *Guidelines 05/2020 on Consent under Regulation 2016/679* version 1.1 (2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[25] World Med. Ass'n, *WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects* (1964), www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/; Council of Eur., *Recommendation No. R(99)4 of the Committee of Ministers to Member States on Principles Concerning the Legal Protection of Incapable Adults* (1999), www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(99)4E.pdf.

[26] Alzheimer Eur., *Understanding Dementia Research*, www.alzheimer-europe.org/research/understanding-dementia-research.

https://doi.org/10.1017/9781009373234.005 Published online by Cambridge University Press

In order to address data protection requirements, we must first identify the controllers and processors involved. In the TeNDER project, we employed fitness wearables in combination with RGB skeleton cameras and microphones, which were placed in different care settings – a retirement home, rehabilitation room in the hospital, day care center, etc. This meant that the user partners, such as health care organizations, were acting as data controllers, since they had determined which tools they would use (*the means*) and what kind of care or therapeutic outcomes (*the purposes*) would be achieved using those means. Technology providers, both external and part of a consortium, acted as data processors, carrying out the instructions given by the controllers. The patients enrolled in the evaluation pilots were recruited by the health care providers and represent the data subjects in this scenario.

To ensure an appropriate techno-legal conversation, the user partners and technology providers (i.e., the controllers and processors) were asked to provide feedback by means of impact assessment questionnaires. Their feedback has informed our approach to solving the specific challenges described below.

B *Specific Challenges of the TeNDER Remote Care Technology*

i Data Sharing with a Third-Party Service Provider

The responsibility of the controller for ensuring compliance with the data protection requirements is complicated by the fact that many RCTs are provided by external providers. To a certain extent, the privacy risks can be mitigated by measures taken by developers and users, including patients, caregivers, and organizations. These counter-measures can help minimize the amount of data processed by external parties when opting out of data sharing is not possible. Normally, the controller and the processor will adopt relevant agreements, such as the controller-processor agreement (art. 28(3)) of the GDPR; however, with external service providers that is sometimes not feasible, and the terms of use/terms of service apply instead.

Data protection in the wearables market calls for special attention as the functionalities of wearables become even more sophisticated and provide for wide-ranging data collection. Personal data of the most intimate nature – activity, moods, emotions, and bodily functions – can be combined with other sources of data, raising such potential harms as discriminatory profiling, manipulative marketing, and data breaches.[27] The lack of data privacy protections could be addressed by a greater adoption of the data protection by design principle and more transparency, especially regarding privacy policies.[28]

[27] Kathryn C. Montgomery et al., Ctr. for Digit. Democracy, *Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection* (2016), www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf.

[28] Id.; T. Mulder & M. Tudorica, Privacy Policies, Cross-Border Health Data and the GDPR, 28 Info. & Commc'n Tech. L. 261 (2019).

https://doi.org/10.1017/9781009373234.005 Published online by Cambridge University Press

At TeNDER pilot sites, we used fitness wearables, such as the Fitbit, to follow up on patients' rehabilitation and daily routines by tracking events such as energy expenditure, sleep, and activity. The wearables were connected to smartphones and tablets, and the data from the wearables was extracted to paint a comprehensive picture of a patient's movement.[29]

The potential access of Fitbit to the data on the device and the wearable, as the service provider, has been identified as a potential challenge. The Fitbit blog provides some tips on enhancing privacy and data protection while using their services, including going incognito, editing the profile and display name, making personal stats (such as birthday, height, and weight) private, hiding badges, and adjusting for different location settings.[30] However, generally opting out of data sharing with the service provider is not possible. Considering the TeNDER project involves very vulnerable populations, additional safeguards were adopted in the process: Setting up dedicated accounts and email addresses, using devices specifically for the project purposes, and avoiding real names or specific dates of birth as much as possible. These safeguards contribute to the implementation of the principle of data minimization, set in art. 5(1)(c) of the GDPR, which is one of the keystones of privacy and data protection by design.[31]

ii Infrared Cameras and Accidental Capture

In the pilots, we plan to use infrared cameras to keep track of patients' rehabilitation processes and to alert the caregiver should the patient fall. However, cameras can accidentally capture other people aside from the patient.

Our approach was based on the GDPR and the opinion of the EDPB.[32] A video system used to process special categories of data must be based on valid legal grounds as well as a derogation under art. 9. Since TeNDER is a research project, informed explicit consent was collected from the patients prior to the data processing. Adopters in a research setting could rely on the derogation of "scientific research purposes" under art. 9(2)(j), where obtaining explicit consent could not be feasibly done. In this regard, it is noteworthy that the GDPR provides that the term research setting

[29] TeNDER, supra note 21.

[30] Danielle Kosecki, 13 Fitbit Community Features You Can Customize for More (or Less!) Privacy, *Fitbit News* (2017), https://blog.fitbit.com/fitbit-privacy-settings/; Danielle Kosecki, Ask Fitbit: How Can I Keep My Stats Private?, *Fitbit News* (2017), https://blog.fitbit.com/go-incognito/.

[31] Nor. Consumer Council, *Consumer Protection in Fitness Wearables* (2016), https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-protection-in-fitness-wearables-forbrukerradet-final-version.pdf; Eur. Data Protection Bd., *Guidelines 4/2019 on Article 25: Data Protection by Design and by Default* version 2.0 (2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[32] Eur. Data Protection Bd., *Guidelines 3/2019 on Processing of Personal Data Through Video Devices* version 2.0 (2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

"should be interpreted in a broad manner, including for example technological development and demonstration." However, since accidental capture can happen to an undefined audience, relying on their consent is not realistic. In the EDPB's opinion,[33] the legitimate interests of the controller are suggested as an alternative legal basis. However, this basis cannot be relied on if the data subject's rights and interests outweigh the legitimate interest. Considering that RCTs involve health data, it is difficult to see how that would meet the legitimate interests balance test.[34]

To avoid accidental capture in the pilot, the infrared cameras, which process skeleton outlines without biometric data or identifying facial characteristics, will only be used in physiotherapy sessions as part of the rehabilitation room pilot.

iii Integration with EHRs

In order to ensure a more comprehensive overview of a patient's medical history, the development phase includes integrating electronic health records (EHRs) into the system. Clinical history will, later in the project, be matched with data from other devices to ensure an integrated care service. In data protection terms, this contributes to the data accuracy principle. This principle requires that personal data must be accurate and, where necessary, kept up to date, and that inaccurate personal data must be erased or rectified without delay (art. 5(1)(d) of the GDPR). Where patient data is concerned, this principle is very important to ensure the appropriate treatment of the patient, especially if data are going to be fed into artificial intelligence (AI) systems.[35]

One of the challenges in the EU is the diversity of EHR data formats in different member states. To this end, the Commission has adopted a "Recommendation on a European Electronic Health Record" (REHR) exchange format.[36] According to its Recital 10, the goal of the REHR is the interoperability of different EHRs and to allow for processing information in a consistent manner between those health information systems, so that the provision of cross-border health care services (including remote care) becomes easier for the patient. REHR is a voluntary interoperability system – member states that sign up should ensure that at least the following data points should be interoperable: Patient summaries, e-prescriptions and e-dispensations, laboratory results, medical imaging and records, and hospital discharge reports (point 11 of the REHR).

[33] Id.

[34] Article 29 Working Party, Eur. Commn', *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC* (2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[35] Studio Legale Stefanelli & Stefanelli, Artificial Intelligence, Medical Devices and GDPR in Healthcare: Everything You Need to Know About the Current Legal Frame, *Lexology* (2022) www.lexology.com/library/detail.aspx?g=8cba1347-0323-4951-b9b5-69015f6e169f.

[36] Eur. Comm'n, *Commission Recommendation of 6.2.2019 on a European Electronic Health Record exchange format* C (2019) 800 final.

Since EHRs involve patient data, the link to the GDPR is clear. To set up the system in accordance with the data protection framework, the development follows the Article 29 Working Party's guidelines on EHR.[37] Even though this document was released on the basis of the Directive 95/46, many of its principles are still relevant under the new regime. Among the recommendations of the document are strong access controls and authentication measures for the patient and the health care professional; further use of information contained in the EHR only for legitimate purposes, such as providing better treatment; and data security and data minimization measures, such as separate storage of especially sensitive data.[38]

The integration of electronic health care records is still in progress, and its legal aspects will be evaluated at the end of the project. The techno-legal collaboration on EHR integration has, so far, focused on two aspects: The mapping of applicable legal frameworks, as described in the above paragraphs, and their take-up by developers in order to build the products.[39]

iv Preliminary Results: Essential Data Protection Requirements for Developing Remote Care Technologies

The main takeaway from our work in the TeNDER project so far can be summarized as a set of essential requirements for potential future developers and users of similar technologies. This is by no means an exhaustive list – as explained above, unlike real-life health care settings, research projects are a controlled environment with highly formalized procedures aimed at developing and testing technologies. In contrast, organizations who adopt RCTs for their own patients may be required to comply with additional obligations, including carrying out a data protection impact assessment as required by art. 35 of the GDPR or adopting processing agreements under art. 28(3), enabling data subject rights requests (especially the right to access) and the portability of health care records, and so on. While the system is being developed in line with the GDPR, future end-users will play a major role in complying with data protection and other sectoral or national laws. An expanded list of the requirements summarized below in Table 3.1 is available in the last legal report of the project, published in April 2023.[40]

[37] Article 29 Working Party, supra note 13.

[38] Id.

[39] TeNDER, D5.3, *First Report on the Health Record and Pathway Gathering* (2021), www.tender-health.eu/project/here-you-can-find-a-selection-of-the-projects-public-deliverables-as-they-become-available/.

[40] TeNDER, *D1.6, "Final Version of Fundamental Rights, Ethical and Legal Implications and Assessment"* (2023), www.tender-health.eu/project/here-you-can-find-a-selection-of-the-projects-public-deliverables-as-they-become-available/.

TABLE 3.1 *Essential data protection requirements for RCTs: Preliminary results of TeNDER*

Role in RCT	*Potential data protection role*	*Essential requirements*
Developers and technology providers	*Potential processors*	Design RCTs according to the principles of data protection by design and by default (art. 25 of the GDPR), especially when different devices and tools are being used, such as in the case of EHR integration. This will also operationalize the principle of data minimization: no other personal data than that which is adequate and relevant to the specific purpose will be processed. If EHR are fed into the system, ensure the data contained in the records are accurate and kept up to date, as per art. 5(1)(d) of the GDPR. Assess whether they are a processor under art. 4(8) of the GDPR (the entity that carries out the processing on behalf of the controller) and take the required measures, such as notifying the controller (the health care organization) about the involvement of other processors (third parties such as external providers of RCTs or other technologies).
Users (health organizations)	*Potential controllers*	Apply technical and organizational measures to ensure general compliance with data protection rules (art. 5(2) and 24 of the GDPR). Ensure valid consent is given. Since many of the patients enrolled in the pilots are experiencing cognitive decline, the information given must be appropriate to the patients' level of understanding. Preferably, a trusted person should be involved in the process of obtaining consent (e.g., a family member or other caregiver). If using cameras or other especially intrusive technologies, consult the patients on their placement within the room, and inform them of the option to turn the device off. Keep data in the EHR accurate and up to date; respond to patient requests for rectification of their medical information.
Users (patients)	*Data subjects*	The onus to maintain data protection and security measures is on the developers and health care organizations, not on the user (the principle of data protection by default). When using third-party devices and opting out of data sharing is desired but not possible (e.g., in the case of wearables), use mitigation measures, such as using pseudonyms instead of names, inputting approximate date of birth, not connecting the device to social media presence, etc.

V CONCLUSION

What do the findings of this chapter mean for the development of RCTs? I have taken a two-pronged approach and discussed the application of selected legal provisions to RCTs in general, against the application of the same provisions to specific technology developed as part of the TeNDER project. While it may not be possible to fully resolve the tension between particular technologies and abstract legal frameworks, in general, knowing how to interpret the law can bring us closer to bridging the gap.

Responding to the data protection challenges of developing RCTs involves both a technological and organizational angle, such as using different tools in appropriate contexts (e.g., cameras in the rehabilitation room rather than in patients' homes), as well as legal solutions (e.g., applying additional safeguards to ensure the informed-ness of the patients' consent). What is acceptable to patients who are receiving remote care in the privacy of their own home, rather than in health care organizations, as well as what kind of technological development is feasible, should be further explored by interdisciplinary, socio-technological-legal research. Nor are all the legal questions resolved, such as the lack of legal provisions under the GDPR that safeguard the consent of persons with cognitive decline. The same problem applies regarding the role of the terms of use of service providers in ensuring that the external processors will comply with the data protection rules.

The scope of this chapter is likewise limited by the scope of the project itself. Since the latter is largely concerned with development, this chapter explores the development process as well, rather than the eventual use of the products in health care organizations after the end of the project. Further, the project will be running for another year, and the results reported in this chapter are preliminary as of the spring of 2022. Legal findings will mature together with the technology, and some of the legal aspects concerning the future use of the TeNDER technologies will be clearer at the end of the development and testing phases.