Proactive Legal Design for Health Data Sharing Based on Smart Contracts

5

Proactive Legal Design for Health Data Sharing Based on Smart Contracts

ARIANNA ROSSI AND HELENA HAAPIO*

I. Introduction: Scripts, Stacks and the Human Side of Smart Contracts

> The technology of smart contracts neglects the fact that people use contracts as social resources to manage their relations. The inflexibility that they introduce, by design, might short-circuit a number of social uses to which law is routinely put.[1]

Smart contracts are increasingly used in contexts where human choice, oversight and flexibility matter. Still, the human side of smart contracts has gained far less scholarly attention than their technical and legal aspects. Karen EC Levy in her article 'Book-Smart, Not Street-Smart' reminds us of the fact that contracts are deeply social tools, as well as legal ones, and of the risks, if smart contracts are not designed to take into account the social complexities of contracting; while they may facilitate technically perfect implementation and lower transaction costs, they fail to understand or integrate the social world and human behaviour.[2]

The social and human aspects are especially present in the use case that this chapter examines: technological architectures that enable the sharing of health data, with a focus on emerging technologies that would allow a multitude of parties to access and process massive biomedical datasets in a secure and decentralised

* The authors would like to thank the anonymous reviewers for their helpful comments and Jim Hazard for his valuable feedback. The authors would also like to aknowledge Leila Hamhoum for her precious editorial assistance.

[1] KEC Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law' (2017) 3 *Engaging Science, Technology, and Society* 1, 1.

[2] ibid 10. 'Automated contracts', according to Levy (ibid) 11, 'tend to focus on contracts' capacity for legal communication, perhaps to the expense of their social capacity'.

manner while providing transparency about such processes and about the permissions granted to specific data uses. This chapter addresses the benefits and challenges related to the construction of user-centric solutions intended to allow individuals to whom the data refers[3] to relinquish rights over their information through the instrument of informed consent. Other parties include researchers and physicians who connect and communicate with those individuals to obtain, collect and use such data; providers of the infrastructure meant to enable the sharing and querying of vast amounts of data; and a variety of organisations, such as research centres, medical institutes and various healthcare facilities that access and analyse that data to enhance the predictive power of their models.[4] To participate in the data sharing economy, these organisations need to comply with applicable laws, for example, by ensuring privacy and transparency of data processing, and adhere to the data permissions established by the participants. In this context, blockchain technologies offer the backbone for the integration with other applications like smart contracts, employed to automate processes, such as participant compensation and real-time data use permissions.

Smart contracts are not necessarily (legal) contracts, especially in our context. Echoing the title of the article by Shaanan Cohney and David A Hoffman, 'Transactional Scripts in Contract Stacks',[5] we might frame them as 'scripts' or 'transactional scripts'. These scripts, which may include consents or permissions, may or may not constitute or be part of (legal) contracts, and they may or may not be human-readable. They seldom stand alone: there is often a 'stack' or a 'chain' (or several stacks or chains) – scripts are the building blocks of contract and consent stacks and chains, which may be quite complex.[6] Given the intricacies of the health data sharing scenario, the expectations and the objectives of the numerous participating stakeholders must be carefully aligned. This complexity calls for proactive legal thinking merged with design thinking, and a legal design intervention based on transparency-enhancing tools.

There is a growing need for easy-to-use solutions, on the one hand, and for complying with operational and legal requirements, on the other. Balancing

[3] In this chapter, the terms 'individuals', 'patients' and '(research) participants' will be used interchangeably. In the context of data privacy, they can also be referred to as 'data subjects'.

[4] TK Mackey, TT Kuo, B Gummadi, KA Clauson, G Church, D Grishin, K Obbad, R Barkovich and M Palombini, '"Fit-for-Purpose?" – Challenges and Opportunities for Applications of Blockchain Technology in the Future of Healthcare' (2019) 17 *BMC Medicine* 68.

[5] S Cohney and DA Hoffman, 'Transactional Scripts in Contract Stacks' (2020) University of Pennsylvania, Institute for Law & Economy Research Paper No. 20-08, available at ssrn.com/abstract=3523515. See also JG Allen, 'Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Languages' (2018) 14 *European Review of Contract Law* 307.

[6] See, eg, the consent receipts (made of machine-readable code and human-readable code) by the Kantara initiative in R Beaumont, C Cooper, S D'Agostino, R Graves, I Henderson, M Hodder, H Honko, A Hughes, T Jones, R Lapes, O Maerz, E Maler, J Pasquale, S Tuoriniemi and J Wunderlich, 'Consent Receipt Specification' (M Lizar and D Turner eds, v1.1.0, Kantara Initiative, 20 February 2018), available at kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0.

the needs and interests of the different stakeholders is not always easy. The researchers, planners, developers, builders and users of complex technologies need support and guidance. Contracts, consents and permissions are not easy to work with, even when they stand alone. The inclusion of code, stacks and chains in our context adds a new layer of complexity to the operational and legal issues. But if we think of smart contracts, consents and permissions as *scripts*, *artifacts*[7] or *things*[8] – human-made products like any others – it becomes easier to approach questions related to their functionality, usability, and *quality by design*.[9] Viewing them as *communicative artifacts* and *information products*[10] highlights the notion that they are human-made instruments that intend to convey information for a purpose. In this way, we can remove much of the mystique around them.[11] It then becomes natural that communicating their contents and ramifications can be informed by contract/legal design scholarship and privacy communication design scholarship.

Proactive legal designers can bring a new perspective by identifying and making different expectations and requirements visible early on, helping to embed them from the beginning into the design specifications, building in navigation tools, affordances and signifiers, and asking questions such as: How can we make contract and consent stacks or privacy communication work better? How can we ensure that the smart contract code or script reflects the intention of the stakeholders and does what it is intended to do – and how might design tools and methods assist in managing and using the data inputs and outputs? How can we secure successful and compliant implementation?

Section II begins by introducing the research scenario and the many benefits and challenges involved in health data-sharing transactions based on smart contracts. Section III begins the path towards finding a balance between the different stakeholders' often conflicting needs and goals, integrating data sharing with dynamic consent models and smart contracts, and embedding transparency into health data sharing architectures. After introducing proactive law and legal design, section IV illustrates, with examples, how these can be merged and brought to practice with the help of design patterns. Section V concludes.

[7] MC Suchman, 'Contracts as Social Artifacts' (2003) 37 *Law & Society Review* 91.

[8] AA Leff, 'Contract as Thing' (1970) 19 *The American University Law Review* 131.

[9] Quality by design is a concept introduced in JM Juran, *Juran on Quality by Design: The New Steps for Planning Quality into Goods and Services* (New York, Free Press, 1992). Juran provides a set of steps that can be used to establish quality goals, identify customers, determine customer needs, provide measurement, and develop process features and controls to improve – all very much in line with the design thinking approach adopted in this chapter.

[10] For information products more generally, see E Orna, *Making Knowledge Visible: Communicating Knowledge through Information Products* (London, Gower Publishing, 2005).

[11] Suchman, 'Contracts as Social Artifacts' (2003) 93. 'By seeing contracts as simply one among many types of artifact that we produce and deploy in our daily lives,' Suchman notes, 'we strip them of their legalistic mystique'.

II. Research Scenario

A. Benefits of Health Data Sharing and Reuse

'The value of data lies in its use and re-use' maintains the 2020 European Commission's Data Strategy.[12] This political statement emphasises the necessity of a data-agile ecosystem for the successful development of a competitive economy meant to create a variety of products and services by the private and public sector alike. In the healthcare sector, access to large databases has tremendous value, as it enhances the predictive power of data analysis and provides insights from population health analytics.[13] Yet many medical centres and research facilities are not able to maintain a set of patient records and other data large enough to develop and train their own predictive models, for instance in the case of rare conditions. This is why there is a growing tendency to recur to shared datasets: not only are opportunities for research advancement distributed to a larger network of parties, with the deriving scientific, social and economic implications, but also the efforts to collect, describe and qualify huge amounts of information are not wasted.

Although the possible applications are several, in the medical sector the example of genome data reuse is particularly telling. Nowadays, people increasingly have their DNA sequenced[14] for many reasons of medical and non-medical nature.[15] The data produced is valuable for a number of (commercial and non-commercial) organisations that aspire to leverage an unprecedented amount and variety of information to establish correlations between genetic traits and conditions, supporting thereby preventive medicine. Moreover, genetic data is one of the keys to personalised healthcare, which promotes more efficient, accurate and targeted treatments and prevention strategies for humankind, while it opens new revenue streams for pharmaceutical companies.

[12] European Commission, 'A European Strategy for Data – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions' COM(2020) 66 final, 6.

[13] Mackey, Kuo, Gummadi, Clauson, Church, Grishin, Obbad, Barkovich and Palombini, '"Fit-for-Purpose?"' (2019).

[14] National Human Genome Research Institute (NHGRI), 'DNA Sequencing Fact Sheet', available at www.genome.gov/about-genomics/fact-sheets/DNA-Sequencing-Fact-Sheet: 'Sequencing DNA means determining the order of the four chemical building blocks – called "bases" – that make up the DNA molecule. The sequence tells scientists the kind of genetic information that is carried in a particular DNA segment', for instance changes in a gene that may cause disease.

[15] Motivations include learning about predisposition to heritable disorders, modelling response to medicinal products, uncovering risk of conceiving children with severe genetic conditions and gaining knowledge about ancestry, familial relationships or personal traits. See SA Garner and J Kim, 'The Privacy Risks of Direct-to-Consumer Genetic Testing: A Case Study of 23andMe and Ancestry' (2018) 96 *Washington University Law Review* 1219, 1236.

However, for such opportunities to flourish, the dominant data governance model constituted by data silos needs to be vanquished. Data silos generate value exclusively for those holding the data, not for those who have provided the data, nor for other market players that could create value with that data. Legislative (eg, the General Data Protection Regulation in the EU) as well as other initiatives (eg, MyData[16]) aim to unlock fair digital competition, by developing novel data ownership and sharing approaches. To encourage the free flow of data and pinpoint alternative data governance models based on data sharing, there is a growing need for consumer-centric tools, such as consent and identity management platforms. Such models aspire to rebalance the existing power asymmetry, by placing the users at the centre of processes, restoring their ability to self-determine the permissible use of their information and transforming merely formal digital rights into easily actionable rights.[17] These include, for example, the right to give and withdraw consent for the information flow and to keep track of the parties accessing one's own data, the purposes for which it is accessed and the outcomes of such activities.

B. Issues Concerning Health Data Sharing and Reuse

Great knowledge, however, comes with a cost. The flow and reuse of personal data, especially sensitive health-related information, ought to be protected through legal and ethical means. For services offered in the EU,[18] not only should organisations be able to put such safeguards in place by adopting adequate technical and organisational measures and integrating them in their workflow *by design and by default*,[19] but they are also required to be able to demonstrate compliance, for

[16] The purpose of MyData Global is to empower individuals by improving their right to self-determination regarding their personal data. See MyData.org, 'About' at mydata.org/about.

[17] MyData.org, 'Declaration' (v1.0), available at mydata.org/declaration. According to the Declaration, 'in many countries, individuals have enjoyed legal data protection for decades, yet their rights have remained mostly formal: little known, hard to enforce, and often obscured by corporate practices. We want true transparency and truly informed consent to become the new normal for when people and organisations interact. We intend access and redress, portability, and the right to be forgotten, to become "one-click rights": rights that are as simple and efficient to use as today's and tomorrow's best online services'.

[18] In the EU, the legal protection of medical as well as other personal data is established by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 (General Data Protection Regulation) [2016] OJ L119/1 (GDPR), which also poses a number of obligations on organisations collecting and processing data, such as the obligation to implement technical and organizational measures to guard the data from harm.

[19] GDPR, Art 25. See also European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (13 November 2019), available at edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

example by maintaining an electronic record of processing activities. Such safeguards should effectively and demonstrably implement data protection principles, including the central tenet of transparency. Transparency aspires to level out information asymmetries and enable the parties providing knowledge about themselves to understand and exert their rights.[20]

Given the value of patient records and the significance of the sector for society, healthcare constitutes one of the favourite attack vectors worldwide. Data breaches can lead to the reidentification of deidentified datasets, exposing patients to the repercussions of data misuse, such as fraudulent activities and discrimination. Healthcare providers may be subject to service disruption, suffer significant financial damage, and face the possibility of litigation.[21] Moreover, a 2019 data breach report[22] observed that the majority of health data losses, theft or accidents due to unauthorised access can be ascribed to internal actors (eg, hospital employees) who either perform unintentional actions exposing vulnerabilities or abuse their authorisations. So the medical sector needs not only to protect itself from external mischievous parties, but also to be vigilant about internal threats, such as human errors in the implementation and enforcement of security policies.[23]

Since information privacy is a non-negotiable precondition for health data analysis, innovative approaches that balance security and confidentiality of personal information with the endavour of keeping high-performance processing capacities are arising. The combination of the respect for user-established rules about permissible data processing and the promotion of transparency about the processing practices is meant to establish a relationship of trust among the stakeholders. Indeed, degradation of trust severely impacts data sharing attitudes and has cascade effects in all data-informed industries.[24] Organisations offering genetic services, for instance, face today intense scrutiny due to questionable practices[25] and yearn to regain people's trust. Enlarging their user base is indispensable to create a prosperous data sharing ecosystem, though. Thus, such organisations have a urgent interest in implementing adequate privacy and security measures as well as user-centric data governance models. Moreover, even business-to-business data sharing lags behind, one reason being 'the lack of trust between economic

[20] European Data Protection Board, 'Guidelines 4/2019' (2019) 14.

[21] A McLeod and D Dolezel, 'Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches' (2018) 108 *Decision Support Systems* 57.

[22] Verizon, '2019 Data Breach Investigations Report' (2019) 44–45, available at enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

[23] R Ayyagari, 'An Exploratory Analysis of Data Breaches from 2005–2011: Trends and Insights' (2012) 8 *Journal of Information Privacy and Security* 33.

[24] See, eg, the Facebook–Cambridge Analytica data misuse scandal, H Tuttle, 'Facebook Scandal Raises Data Privacy Concerns' (2018) 65 *Risk Management* 6.

[25] For instance, recent cases of access to consumer genomics services and their databases by law enforcement agencies with the objective of investigating unsolved crimes and the acquisition of genetic data by biopharmaceutical companies to develop new drugs without users' consent or awareness have raised consumers' and authorities' concerns. Garner and Kim, 'The Privacy Risks of Direct-to-Consumer Genetic Testing' (2018) 1221–22.

operators that the data will be used in line with contractual agreements'.[26] Lack of clarity and transparency of the contractual conditions concerning digital services stifles economic development of micro, small and medium enterprises.[27]

III. Seeking a Balance – Identifying, Aligning and Managing Expectations

A. Complexity Caused by the Stakeholders' Conflicting Needs and Goals

In health data sharing scenarios,[28] an elaborate mix of needs and objectives of the various parties is at stake. In user-centric services, individuals impose rules about the permissible use of their data to the organisations collecting or processing the data, often through the instrument of consent. As for the organisations maintaining datasets or providing the sharing infrastructure, they need to establish data governance rules and oversight mechanisms,[29] for instance by clarifying the terms of use of their services and the privacy practices towards the individuals, while also delineating the safeguards under which other parties (eg, research centres) access and process their information. To regulate such access, organisations make data sharing agreements encompassing patients' permissions as well as rules regarding legitimate use of data (eg, in terms of security policies). The research institutes, in turn, need to ensure that their employees respect regulatory requirements as well as their internal privacy and security policies that more or less closely mirror the data sharing agreements. Given the sensitivity of the type of data at hand and the cascade effects of a breach of trust, it is of utmost importance that the expectations pinpointing data sharing among these different actors are clearly set and respectfully honored.

This scenario suggests an intricate process of multi-channel information provision and dynamic consent requests. This ecosystem is even more complicated: it may need to support a blend of analogic and digital means to collect, process and manage the data, as well as to provide information that is necessary for the establishment of the consent and contract relations and their impact. For instance, patients might simultaneously interface with their human healthcare provider as well as with mobile applications and sensors, without necessarily needing to grasp

[26] COM(2020) 66 (n 12) 7.

[27] European Commission, Study on the Economic Detriment to Small and Medium-Sized Enterprises Arising from Unfair and Unbalanced Cloud Computing Contracts – Final Report (European Commission Directorate-General for Justice and Consumers, November 2018) 46–49.

[28] For a review, see C Suver, A Thorogood, M Doerr, J Wilbanks and B Knoppers, 'Bringing Code to Data: Don't Forget Governance' (2020) *Journal of Medical Internet Research* 2.

[29] ibid 2.

the complexity of the underlying sharing architecture. It becomes pivotal, then, to design the appropriate affordances to enable desirable interactions and to foster shared values while inhibiting detrimental actions.

B. Integrating Data Sharing on the Blockchain with Dynamic Consent Models and Smart Contracts

Blockchain technologies are increasingly proposed as solutions to challenges concerning privacy, transparency and accountability for health data sharing.[30] The promoters of such solutions underline the advantages of sharing healthcare datasets without the necessity of trusting a third-party cloud.[31] The adoption of blockchain-based solutions is also intended to successfully manage different stakeholders' needs emerging from labyrinthine data sharing architectures while ensuring confidentiality and verifiability of the information. It is claimed that this digital architecture is able to 'ensure the resilience, provenance, traceability, and management of health data'[32] which originates from a variety of sources, including different data providers, but also manifold devices and sensors (eg, various data produced in the Internet of Medical Things[33]).

The distribution of the data on various databases and machines (ie, nodes) renders the history of transactions immutable and tamper-resistant, thus offering an audit trail.[34] Moreover, the information stored on the blockchain can be secured through advanced encryption schemes.[35] A private ledger (ie, a private network including a limited number of trusted participants) can transparently keep a record of all data access requests and permissions, establishing accountability and allowing patients to scrutinise access to their data. Smart contracts can be conceived to automate the verification of the medical professional accreditation and licensure of participants,[36] thereby ensuring that only parties with verified identities are authorized to engage in data processing activities.

[30] Mackey, Kuo, Gummadi, Clauson, Church, Grishin, Obbad, Barkovich and Palombini (n 4) 12; M Mettler, 'Blockchain Technology in Healthcare: The Revolution Starts Here,' in *2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)* (IEEE 2016) 1–3, available at doi.org/10.1109/HealthCom.2016.7749510; X Yue, H Wang, D Jin, M Li and W Jiang, 'Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control' (2016) 40 *Journal of Medical Systems* 217, available at doi.org/10.1007/s10916-016-0574-6.

[31] B Shen, J Guo and Y Yang, 'MedChain: Efficient Healthcare Data Sharing via Blockchain' (2019) 9 *Applied Sciences* 3, available at doi.org/10.3390/app9061207.

[32] Mackey, Kuo, Gummadi, Clauson, Church, Grishin, Obbad, Barkovich and Palombini (n 4) 1.

[33] GJ Joyia, RM Liaqat, A Farooq and S Rehman, 'Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain' (2017) 12 *Journal of Communications* 240.

[34] WJ Gordon and C Catalini, 'Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability' (2018) 16 *Computational and Structural Biotechnology Journal* 227, available at doi.org/10.1016/j.csbj.2018.06.003.

[35] Mackey, Kuo, Gummadi, Clauson, Church, Grishin, Obbad, Barkovich and Palombini (n 4) 1; Yue, Wang, Jin, Li and Jiang, 'Healthcare Data Gateways' (2016) 218.

[36] Mackey, Kuo, Gummadi, Clauson, Church, Grishin, Obbad, Barkovich and Palombini (n 4) 6–7.

Furthermore, patients can use smart contracts to assign digital access rules to their data and embed policies designed to implement those rules,[37] like limiting the access period.[38] Thus, consent traceability is facilitated, since registering authorisations on a permissioned blockchain allows identity verification of the entities viewing or retrieving the data. Their access to specific records can be automatically granted, refused or revoked by the rules established by patients themselves, which would enable easier sharing.[39] Automated notifications can be sent to the parties providing the data, to warn them of recent data accesses or inform them about new data sharing opportunities.[40] These functionalities are crucial for the implementation of dynamic consent models, which enable patients to negotiate in a continuous and nuanced manner the authorized use of their data by certain organisations and for certain activities through time. For instance, people might want to provide new consent to new research activities that were not foreseen at the time of registration or revoke their consent permissions due to changing circumstances.[41]

For these promising models to gain traction, it is necessary to move away from a conceptualisation of consent as a single-point transaction. Digital consent (ie, e-consent) applications[42] play a major role in a feasible micro-management of users' choices and are growing in number and purpose in the biomedical research domain. Their integration with smart contracts embeds the promise of promoting a decentralised data marketplace, where health data sharing can be accelerated by compensating the participants who provide precious information about themselves,[43] yet are traditionally excluded from any benefit (eg, financial

[37] For example, a policy may enforce that separate transactions representing consent are sent from both patients and care providers, before granting viewing permissions to a third party. A Azaria, A Ekblaw, T Vieira and A Lippman, 'MedRec: Using Blockchain for Medical Data Access and Permission Management' in I Awan and M Younas (eds), *2016 2nd International Conference on Open and Big Data (OBD 2016)* (Institute of Electrical and Electronics Engineers IEEE, 2016) 27, available at ieeexplore.ieee.org/document/7573685.

[38] Gordon and Catalini, 'Blockchain Technology for Healthcare' (2018) 227.

[39] ibid 227.

[40] Automated notifications based on smart contracts are employed to warn healthcare providers within the IoT-enabled automated patient monitoring. AD Dwivedi, G Srivastava, S Dhar and R Singh, 'A Decentralized Privacy-Preserving Healthcare Blockchain for IoT' (2019) 19 *Sensors* 7, available at dx.doi.org/10.3390/s19020326.

[41] I Budin-Ljøsne, HJ Teare, J Kaye, S Beck, HB Bentzen, L Caenazzo, C Collett, F D'Abramo, H Felzmann, T Finlay and MK Javaid, 'Dynamic Consent: A Potential Solution to Some of the Challenges of Modern Biomedical Research' (2017) 18 *BMC Medical Ethics* 3.

[42] See, for instance, DB Thiel, J Platt, T Platt, SB King, N Fisher, R Shelton and SL Kardia, 'Testing an Online, Dynamic Consent Portal for Large Population Biobank Research' (2015) 18 *Public Health Genomics* 26; HJA Teare, M Morrison, EA Whitley and J Kaye, 'Towards "Engagement 2.0": Insights from a Study of Dynamic Consent with Biobank Participants' (2015) *Digital Health* (online), available at doi.org/10.1177/2055207615605644. For a review of eConsent in mobile research applications, refer to S Moore, AM Tassé, A Thorogood, I Winship and M Doerr, 'Consent Processes for Mobile App Mediated Research: Systematic Review' (2017) 5 *JMIR mHealth and uHealth* e126, available at doi.org/10.2196/mhealth.7014.

[43] D Grishin, K Obbad, P Estep, K Quinn, SW Zaranek, AW Zaranek, W Vandewege, T Clegg, N César, M Cifric and G Church, 'Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation' (2018) 1 *Blockchain in Healthcare Today* 1.

benefits, but also return about one's contribution to a study). Transactions established in smart contracts can automate certain processes upon the meeting of predefined conditions. In the given scenario, a research institute can demand access to the decentralised database to query certain data; the data subject is enabled to grant the access, provided that adequate compensation is received; details about the different parties and the transaction are recorded on the blockchain; finally, the research institute is admitted to examine the requested data.[44] Such transactions can be established and multiplied with several organisations accessing the data for their own purposes since the contractual conditions are executed automatically. At the same time, the individual retains control over her data. All transactions are registered on the blockchain and are thereby accessible and transparent.

C. Embedding Transparency into Health Data Sharing Architectures

The complex ecosystem where manifold transactions can be automatically enabled by smart contracts contributes, at least in principle, to establish greater transparency about healthcare data use towards the many parties involved. However, the mere fact of building such a verifiable and traceable architecture does not automatically translate into understandable communications, easily applicable instructions and smooth transactions for human beings. Quite the contrary: automation per se does not guarantee the concretisation of values, such as usability, transparency, compliance or trust. For instance, unclear, cumbersome or abstract security policies might cause employee non-compliant behaviour with the measures and, therefore, data breaches.[45]

Truly informed consent is hindered by the complex mix of legal, medical and technical information through which participants need to orientate themselves when they make decisions about data sharing permissions without the guidance of a practitioner. The manner in which such interactions are laid down can ensure transparency and promote trust, and thereby encourage and increase data sharing willingness – or, to the contrary, demolish them. It all depends on the conscious embedding of values into the design of technologies and interactions, beyond pure functional requirements. Our previous work[46] proposed to apply scholars' reflections about the role and responsibilities of code-writers, engineers and designers in shaping people's digital choices and enabling digital rights[47] to the design of legal

[44] ibid.

[45] For examples of data breaches and related reports, see section II.B.

[46] A Rossi and H Haapio, 'Proactive Legal Design: Embedding Values in the Design of Legal Artefacts' in E Schweighofer, F Kummer and A Saarenpää (eds), *Internet of Things. Proceedings of the 22nd International Legal Informatics Symposium IRIS 2019* (Bern, Editions Weblaw, 2019).

[47] 'As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed;

artefacts. The function of designers and engineers is that of 'choice architects':[48] they organise (digital or physical) environments with the intent of guiding people's actions towards predetermined outcomes.[49]

In data-driven environments, the way options are designed and presented to users has the power of promoting or, on the contrary, discouraging desirable behaviours. For example, consent dialog defaults can be designed to stimulate either privacy-preserving practices or privacy-adverse behaviours (eg, minimal versus maximal data sharing). Legal-medical communication can also be designed to attract attention and foster understanding and engagement of the reader[50] or, on the contrary, be willingly or unwillingly arranged to confuse, dishearten and alienate.[51] In both examples, only the first design promotes the value of transparency into the information and the choices presented to users,[52] establishing a connection with the values of fairness, accountability, trust and autonomy.

The sharing of healthcare data poses complex challenges that are variously related to transparency. Transparency-enhancing technologies (TETs),[53] among which we include legal design patterns, offer operational ways to promote transparency, informed consent and other legal-ethical principles into applicable solutions. Given the complexity of the scenario, it is paramount that the expectations of the various stakeholders are aligned and satisfied. This is where merging proactive legal design with user-centric data management and distributed ledger technologies shows its potential.

the extent to which access will be guaranteed. They are the ones who set its nature.' L Lessig, *Code: And Other Laws of Cyberspace* (New York, Basic Books, 1999) 79.

[48] W Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, Mass, Harvard University Press, 2018) 35.

[49] 'Design decisions establish power and authority in a given setting. They influence societal norms and expectations. When people say they use modern information technologies, what they are really doing is responding to the signals and options that the technology gives them. […] Each design decision reflects an intent as to how information technology is to function or be used.' ibid 8.

[50] A Rossi and G Lenzini, 'Transparency by Design in Data-Informed Research: A Collection of Information Design Patterns' (2020) 37 *Computer Law & Security Review* 1, available at doi.org/10.1016/j.clsr.2020.105402.

[51] On embedding transparency into privacy communication design, see Rossi and Haapio, 'Proactive Legal Design' (2019) 541 and A Rossi, R Ducato, H Haapio and S Passera, 'When Design Met Law: Design Patterns for Information Transparency' (2019) 122–123 *Droit de la Consommation – Consumenterecht DCCR* 79.

[52] The second designs, on the contrary, can be defined as 'dark patterns', ie, design choices that coerce, steer or deceive users into making decisions that are not in their best interest. Definition adapted from A Mathur, G Acar, MJ Friedman, E Lucherini, J Mayer, M Chetty and A Narayanan, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 *Proceedings of the ACM on Human-Computer Interaction* 81, available at doi.org/10.1145/3359183. See also eg, R Chatellier, G Delcroix, E Hary and C Girard-Chanudet, 'Shaping Choices in the Digital World. From Dark Patterns to Data Protection: The Influence of UX/UI Design on User Empowerment' (Gwendal Le Grand ed, Commission Nationale de l'Informatique et des Libertés CNIL, 2019).

[53] C Zimmermann, 'A Categorization of Transparency-Enhancing Technologies' (v2, last revised 22 July 2015), available at arxiv.org/abs/1507.04914v2.

IV. Proactive Legal Design in Action

A. Merging Proactive Legal Thinking with Design Thinking

For decades, doctors and lawyers have been viewed as professionals serving an *ex post* function: you get sick, you see a doctor. You have a legal problem, you see a lawyer. The need for such services continues, but reactive care is no longer the only alternative. Instead, many health care and legal professionals now work proactively, *ex ante*, participating in the planning or building of new systems or solutions, promoting clients' chances of success and preventing unnecessary problems. In the legal field in Europe, this is known as practicing proactive law;[54] in the US, preventive law.[55] On both sides of the Atlantic, it can also be framed as practicing proactive legal design.[56]

Unlike legal design, which was added to scholars' and practitioners' vocabulary only recently,[57] proactive and preventive lawyering is not new: preventive law originates from the 1950s and proactive law from the 1990s.[58] These approaches, along with collaborative law and similar disciplines, can be viewed as part of a larger movement in law.[59] These approaches differ from conventional legal research and practice, where the focus is mainly on the past – their focus is on the future. Instead of merely looking back to resolve problems that have already occurred, they look forward to enabling desirable outcomes and prevent the causes of problems from arising. They look beyond legal rules, rights and obligations and focus on goals, needs and relationships, seeking to increase awareness, engagement and clarity as to rights and obligations.[60]

[54] See, eg H Haapio, 'Introduction to Proactive Law: A Business Lawyer's View' in P Wahlgren (ed), *A Proactive Approach* (Stockholm, Scandinavian Studies in Law vol 49, Stockholm Institute for Scandinavian Law, 2006); GJ Siedel and H Haapio, 'Using Proactive Law for Competitive Advantage' (2010) 47 *American Business Law Journal* 641; G Siedel and H Haapio, *Proactive Law for Managers: A Hidden Source of Competitive Advantage* (London, Gower 2011); G Berger-Walliser, 'The Past and Future of Proactive Law: An Overview of the Development of the Proactive Law Movement' in G Berger-Walliser and K Østergaard (eds), *Proactive Law in a Business Environment* (Copenhagen, DJØF Publishing, 2012).

[55] See, eg LM Brown, *Preventive Law* (New York, Prentice-Hall, 1950); LM Brown, *Lawyering through Life – The Origin of Preventive Law* (Buffalo, Fred B Rothman & Co, 1986); TD Barton, *Problem Solving and Preventive Law: Lawyering for the Future* (Lake Mary FL, Vandeplas Publishing, 2009).

[56] See, eg Rossi and Haapio (n 46). See also 'Legal Design Alliance' at www.legaldesignalliance.org.

[57] See, eg G Berger-Walliser, TD Barton and H Haapio, 'From Visualization to Legal Design: A Collaborative and Creative Process' (2017) 54 *American Business Law Journal* 347; CR Brunschwig, *Visualisierung von Rechtsnormen – Legal Design* (Zurich, Schulthess Juristische Medien, 2001).

[58] For the origins of the approaches, see the resources mentioned in notes 54–57.

[59] See S Daicoff, 'Law as a Healing Profession: The "Comprehensive Law Movement"' (2005) 6 *Pepperdine Dispute Resolution Law Journal* 1. Daicoff views approaches such as collaborative law; creative problem solving; holistic justice; preventive law; procedural justice; restorative justice; therapeutic jurisprudence; and transformative mediation as 'vectors' of a movement she calls 'comprehensive law'.

[60] ibid. See also S Daicoff, 'The Comprehensive Law Movement: An Emerging Approach to Legal Problems' in P Wahlgren (ed), *A Proactive Approach* (Stockholm, Scandinavian Studies in Law vol 49, Stockholm Institute for Scandinavian Law, 2006).

For a long time, the proponents of proactive law have called for improved legal communication, services and solutions, with the goal of making these more functional, useful and usable. Before the advent of legal design, designers and lawyers lacked access to each others' mindsets, tools and methods. When design met law,[61] reform-minded legal thinkers and designers became natural allies, increasingly drawn into each others' competencies.[62] Mindsets, tools and processes from design started to be adopted across legal fields, from practice to activism to policy-making.[63]

Computer scientists, too, have identified challenges and roadblocks to widespread smart contract adoption and have started to look for new tools and solutions: current smart contracts need programmers, and they cannot be easily generated or understood. Better interfaces and editors are explored to simplify smart contract generation, enabling them to be created by untrained users, without involving programmers and improving their understandability in order to build confidence that the contract does what is intended.[64] In different parts of the world, computer scientists and lawyers alike have started to look for ways to join forces to make smart contracts 'wise'[65] or 'computable':[66] readable and understandable by both humans and computers.

The time has come to merge proactive legal thinking with design thinking and, with the help of technology, to bring them to practice. Putting the user at the centre, we can integrate lawyers' traditional tools, such as templates[67] and clause libraries, with those of designers and technologists, such as design patterns, both at the code level and at the user interface level.

[61] See Rossi and others, 'When Design Met Law' (2019).

[62] For the developments, opportunities and dangers, see A Perry-Kessaris, 'Legal Design for Practice, Activism, Policy, and Research' (2019) 46 *Journal of Law and Society* 185.

[63] ibid. See also A Perry-Kessaris, 'Work in Progress: Doing Socio-Legal Research in Design Mode' (*Approaching Law*, 28 November 2019), available at amandaperrykessaris.org/2019/11/28/work-in-progress-doing-socio-legal-research-in-design-mode.

[64] K Purnell and R Schwitter, 'Towards Declarative Smart Contracts' in *The 4th Symposium on Distributed Ledger Technology* (Griffith University, 10 December 2019) 18, available at symposium-dlt.org/SDLT2019-FinalProceedings.pdf.

[65] J Hazard and H Haapio, 'Wise Contracts: Smart Contracts that Work for People and Machines' in E Schweighofer, F Kummer, W Hötzendorfer and C Sorge (eds), *Trends and Communities of Legal Informatics. Proceedings of the 20th International Legal Informatics Symposium IRIS 2017* (Wien, Österreichische Computer Gesellschaft, 2017).

[66] See, eg J Cummins and C Clack, 'Transforming Commercial Contracts through Computable Contracting' (University College London, 23 March 2020), available at arxiv.org/abs/2003.10400 and, more generally, the UCL Computable Contracts research page (www.ucl.ac.uk/computer-science/research/research-groups/financial-computing-and-analytics/computable-contracts), identifying legal design for contracts as one of the four key areas to be addressed in order to achieve the vision.

[67] For open-access templates, see, for example, the Lambert Toolkit containing university and business collaboration agreements, including, a fast-track model agreement produced by Public Health England to evaluate potential treatment options for Ebola and Zika very rapidly and to share the results with stakeholders for a coordinated global response; see Intellectual Property Office, 'University and business collaboration agreements: Lambert Toolkit' (Gov.uk, 6 October 2016, last updated 3 April 2019), available at www.gov.uk/guidance/university-and-business-collaboration-agreements-lambert-toolkit. For data sharing agreements and informed consent templates, various forms can be found doing a Google search on the Internet.

B. Design Patterns: Bringing Proactive Legal Design to Practice

When communicating and handling complex legal, technical and medical information, it is important to consider what the users are trying to achieve, and then present information in such a way that the users know what they are expected to do and not do. In order to ensure that users can find and act upon the information, a balance needs to be found between functionality and precision, and between precision and ease of use. According to David Sless, communicating organisations often ask the wrong question: 'They ask, "What information should go into the document?," when they should be asking, "What actions should people be able to perform, easily and quickly, with the information given?"'[68]

After finding the answer, what do designers do? They know that if people do not read the information, find what they need or understand what they find, inadvertent non-compliance will occur. Readers' (and non-readers') problems easily become writers' problems: avoidable complexity causes unnecessary risks. To protect people against themselves and prevent cognitive accidents, designers seek to simplify the user experience. There are three main building blocks to simpler communication: 1) empathise with the users' needs and expectations; 2) distill the communication, boil it down to its essence; and 3) clarify.[69]

Designers seeking clear communication do not overwhelm people with too much information. Instead, they guide them through it, making sure people can skim through headings and sections and easily find relevant information. They explain procedures in a step-by-step fashion and with the help of explanatory diagrams. They use companion icons and clear and visible headings that answer or anticipate typical user questions, and so on. These information design techniques need not be reinvented – they can be identified, shared and reused as design patterns.

i. The Goal of Design Patterns

In recent years, on several continents, researchers and practitioners have started to explore new ways of presenting complex legal information, for example, in the context of contracts[70] and privacy communication,[71] seeking to make legal

[68] D Sless, 'Designing Documents for People to Use' (2018) 4 *She Ji: The Journal of Design, Economics, and Innovation* 125, 131.

[69] See A Siegel and I Etzkorn, *Simple: Conquering the Crisis of Complexity* (New York, Twelve, 2013).

[70] See, generally, G Berger-Walliser, RC Bird and H Haapio, 'Promoting Business Success through Contract Visualization' (2011) 17 *The Journal of Law, Business & Ethics* 55; H Haapio, *Next Generation Contracts: A Paradigm Shift* (Helsinki, Lexpert Ltd, 2013); TD Barton, G Berger-Walliser and H Haapio, 'Contracting for Innovation and Innovating Contracts: An Overview and Introduction to the Special Issue' (2016) 2 *Journal of Strategic Contracting and Negotiation* 3; H Haapio and TD Barton, 'Business-Friendly Contracting: How Simplification and Visualization Can Help Bring It to Practice' in K Jacob,

communication simpler, more accessible and actionable.[72] Design patterns and pattern libraries offer a systematic way to identify, collect, and share good practices. In essence, design patterns are reusable solutions to a commonly occurring problem: something that practitioners can develop, collect and share. Pattern libraries, in turn, are collections or catalogues of patterns.

The original idea of design patterns stems from Christopher Alexander and others,[73] who collected reusable architectural solutions. The idea was later applied to the digital world and gained widespread acceptance with Erich Gamma and others.[74] Since then, design patterns have been extensively used in many other fields, including computer science and interface and UX design.[75] Over the last few years, design patterns and pattern libraries have even made their way to contract design,[76] privacy design[77] and legal design.[78]

D Schindler and Strathausen (eds), *Liquid Legal: Transforming Legal into a Business Savvy, Information Enabled and Performance Driven Industry* (New York, Springer International, 2017); S Passera, *Beyond the Wall of Contract Text: Visualizing Contracts to Foster Understanding and Collaboration within and across Organizations* (Aalto, Aalto University, 2017); H Haapio, R De Rooy and T D Barton, 'New Contract Genres' in E Schweighofer, F Kummer, A Saarenpää and B Schafer (eds), *Data Protection / LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS 2018* (Bern, Editions Weblaw, 2018).

[71] See, generally, Rossi, Ducato, Haapio and Passera (n 51), with references.

[72] Margaret Hagan, the Director of the Legal Design Lab at Stanford Law School, has collected different models to present complex legal information, see 'Examples of Legal Communication Designs' in Stanford Legal Design Lab, 'Legal Communication Design', available at www.legaltechdesign.com/communication-design, and generally, M Hagan, 'Law by Design', available at www.lawbydesign.co.

[73] C Alexander, *A Pattern Language: Towns, Buildings, Construction* (Oxford, Oxford University Press, 1977).

[74] E Gamma, R Helm, R Johnson and J Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software* (Upper Saddle River NJ, Addison-Wesley, 1995).

[75] See, eg J Tidwell, *Designing Interfaces*, 2nd edn (Sebastopol CA, O'Reilly Media, 2014); selected patterns from the book are featured at designinginterfaces.com/patterns.

[76] H Haapio and M Hagan, 'Design Patterns for Contracts' in E Schweighofer, F Kummer, W Hötzendorfer and G Borges (eds), *Networks. Proceedings of the 19th International Legal Informatics Symposium IRIS 2016* (Vienna, Österreichische Computer Gesellschaft, 2016); R Waller, J Waller, H Haapio, G Crag and S Morrisseau, 'Cooperation Through Clarity: Designing Simplified Contracts' (2016) 2 *Journal of Strategic Contracting and Negotiation* 48, 64–65; H Haapio and S Passera, 'Contracts as Interfaces: Exploring Visual Representation Patterns In Contract Design' in DM Katz, R Dolin and MJ Bommarito and R Dolin (eds), *Legal Informatics* (Cambridge, Cambridge University Press, forthcoming). See also International Association for Contract & Commercial Management (IACCM), S Passera and H Haapio, 'IACCM Contract Design Pattern Library, available at contract-design.iaccm.com; and Stanford Legal Design Lab, 'Contract Design Pattern Library' www.legaltechdesign.com/communication-design/legal-design-pattern-libraries/contracts.

[77] H Haapio, M Hagan, M Palmirani and A Rossi, 'Legal Design Patterns for Privacy' in E Schweighofer, F Kummer, A Saarenpää and B Schafer (eds), *Data Protection/LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS 2018* (Bern, Editions Weblaw, 2018); Rossi and Lenzini, 'Transparency by Design in Data-Informed Research' (2020). See also Stanford Legal Design Lab, 'Privacy Design Pattern Library', available at www.legaltechdesign.com/communication-design/legal-design-pattern-libraries/privacy-design-pattern-library. For privacy interface design and data permission design in the context of this chapter, see, eg, Sage Bionetworks, 'Privacy Policy' (Privacy Toolkit), available at designmanual.sagebionetworks.org/privacy-policy.html.

[78] For an overview of legal design patterns, see, eg Rossi, Ducato, Haapio and Passera (n 51). See also Stanford Legal Design Lab, 'Legal Design Pattern Libraries', available at www.legaltechdesign.com/communication-design/legal-design-pattern-libraries.

Consider a situation where the goal is to impact, guide and support decisions and actions, for example at the participant onboarding state. For research to succeed, researchers need to meet participants' concerns and design experiences that pinpoint transparency, autonomy and trust.[79] Here a genre shift from legal documents to user guides can help. User guides are organised around practical tasks, to support action.[80] With the help of technology, static user guides can be turned to apps, playbooks and interactive self-help solutions.[81]

In recent years, new resources have become available that help researchers make decisions about how and when to collect and use data about people and effectively communicate their related messages. Sage Bionetwork provides biomedical researchers with a privacy toolkit of design tools and patterns with accompanying use cases to assist them in using the appropriate patterns in their mHealth and other applications.[82] Another valuable resource is offered by IF, providing a curated catalogue of design patterns ('data patterns').[83] Similarly, design patterns ('multimedia components') for eConsent applications have been gathered[84] to promote informed decision-making about participation in clinical research studies, with the secondary goal of gaining a better insight into the participant experience to improve it.[85] By using design patterns at the appropriate time, participants are helped to understand the types of data that are being collected and how they have the ability to change their data sharing permission, with the goal of building a trusted partnership between researchers and participants.[86]

[79] For further scenarios and helpful design patterns in the context of mobile health research, see V Barone, W MacDuffie, Y Guan and S Simon, 'The Privacy Toolkit for Mobile Health Research Studies – Providing Biomedical Researchers with A Catalog of Privacy Design Patterns for Their Digital Studies' (Privacy Forecast, 2019), available at privacy.shorensteincenter.org/mobilehealth. See also S Moore and M Doerr, 'The Elements of Informed Consent. A Toolkit' (M Doerr ed, v3.0, Sage Bionetworks 2019), available at sagebionetworks.org/wp-content/uploads/2020/01/SageBio_EIC-Toolkit_V3_21Jan20_final.pdf.

[80] User guide format is one of the design patterns included in the IACCM Contract Design Pattern Library. See IACCM, S Passera and H Haapio, 'User Guide Format' (IACCM Contract Design Pattern Library), available at contract-design.iaccm.com/user-guide-format. Good user guides often apply other design patterns included in the Pattern Library; for example, clear layout, skimmable headings, numbered steps, companion icons, icon systems and other visualisations. See IACCM, S Passera and H Haapio, 'Pattern Families' (IACCM Contract Design Pattern Library), available at contract-design.iaccm.com/families-overview.

[81] See, eg H Haapio, 'Legal Design in Action: From Text-Only Guidebooks to Digital, Visual Playbooks' in E Schweighofer, F Kummer and A Saarenpää (eds), *Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS 2019* (Bern, Editions Weblaw, 2019).

[82] Sage Bionetworks, 'Privacy Toolkit for Mobile Health Research Studies', available at sagebionetworks.org/tools_resources/privacy-toolkit-for-mobile-health-research-studies; Sage Bionetworks, 'Informed Consent' (Privacy Toolkit), available at designmanual.sagebionetworks.org/informed-consent.html.

[83] IF, 'Data Patterns Catalogue', available at catalogue.projectsbyif.com.

[84] TransCelerate Biopharma Inc, 'EConsent: Implemetation Guidance Version 1.0' (2017), available at www.transceleratebiopharmainc.com/wp-content/uploads/2017/11/eConsent-Implementation-Guidance.pdf.

[85] ibid 7.

[86] See, eg Barone, MacDuffie, Guan and Simon, 'The Privacy Toolkit for Mobile Health Research Studies' (2019).

ii. Examples of Design Patterns

One of the main goals of design patterns is to share solutions enabling users to notice, explore, retain and interact with information. The selection of patterns needs to be based on what is suited to express a certain communicative goal for a particular user group in a particular context. For those in charge of producing information, the focus changes from clear and concise writing or drafting to *designing communication experiences* with and for multiple user groups. This also involves responding to and balancing different needs and requirements.

The following sections summarise three *experience design patterns* that can be employed for health data sharing to foster transparency, accountability, autonomy and trust.

a. Navigable eConsent Process[87]

Scenario: Consider a participant who has adhered to the biomedical data sharing model under exploration. Before being able to make her record available for a new research activity, she is required to provide informed consent via the dedicated mobile application. She needs to prove that she has understood the reason why and by whom her data will be analysed, the inherent benefits and risks and her rights as both a research participant and a data owner.

Problem: The consent process can be long, complex and information-heavy, while choices can, as a result, be unclear and overwhelming. Moreover, the traditional researcher's additional explanations and comprehension assessment must be remotely self-administered.[88]

Solution: Informed consent is conceptualised as a whole informative process, turning a legalistic form into an engaging and easy-to-navigate experience that drives the participant to a decision that can be described as informed. This translates into breaking down the consent process into different stages, giving an overview of the various steps of the consent process before it starts, and combining simple text with images, videos or other visual means[89] to support comprehension in each phase. The navigation of the participant is thereby supported through the various informative stages until she lands on the actual options for data use authorisation. An assessment of the participant's understanding can also be devised as a precondition that, when met, automatically activates the possibility to grant consent.

[87] Sage Bionetworks, 'Informed Consent' (n 82).

[88] Moore, Tassé, Thorogood, Winship and Doerr, 'Consent Processes for Mobile App Mediated Research' (2017).

[89] eg, comics, see WM Botes, 'Visual Communication as a Legal-Ethical Tool for Informed Consent in Genome Research Involving the San Community of South Africa' (doctoral thesis, University of South Africa, 15 November 2017). See a portion in Rossi and Lenzini (n 50) 12–13.

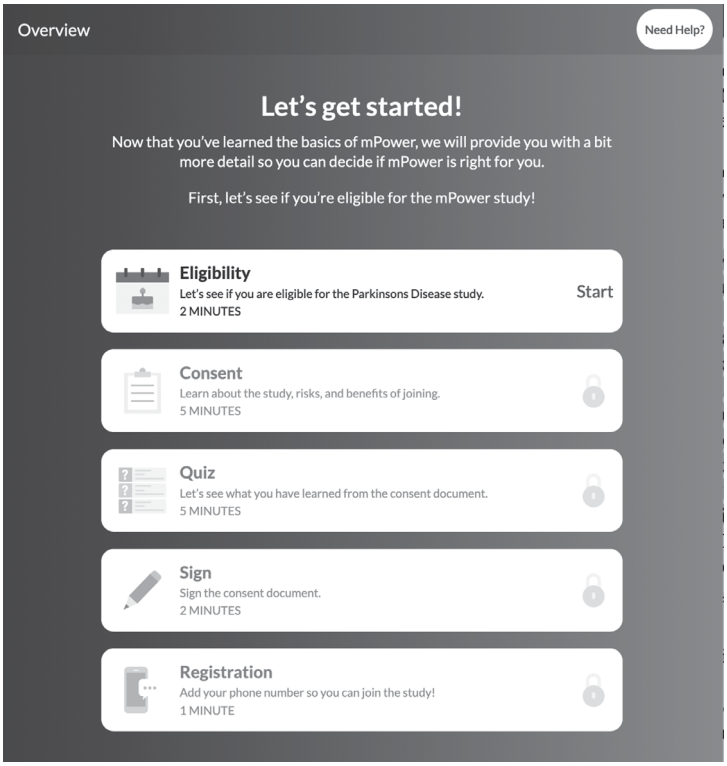

Figure 5.1 eConsent steps for participation in a research study on Parkinson's disease[90]

b. Just-in-time, Dynamic Data Use Permissions[91]

Scenario: Consider a research institute that intends to access its patients' sensitive data collected by IoT devices and sensors and combine it with other data, eg, the patients' medical history already retrieved. Researchers need to send a timely request to the patients where they ask permission to activate sensors and start information collection.

Problem: In traditional consent models, information about possible data uses is provided at a single point in time (eg, at registration), rendering it ineffective for the understanding of the consent options[92] in future uses. Permission options that are not clearly relevant for the task at hand (eg, activating a sensor at the time

[90] Sage Bionetworks, 'Overview' (mPower 2.0), available at parkinsonmpower.org/study/overview. Used with permission.

[91] Sage Bionetworks, 'Just-in-Time Permission' (Privacy Toolkit), available at designmanual.sagebionetworks.org/just-in-time-permission.html.

[92] F Schaub, R Balebako, AL Durity and LF Cranor, 'A Design Space for Effective Privacy Notices' in *SOUPS 2015 Proceedings of the Eleventh Symposium On Usable Privacy and Security* (USENIX 2015) 6, available at www.usenix.org/sites/default/files/soups15_full_proceedings.pdf.

of registration) might be found invasive and cause distrust. They might alienate people from participation or nudge them to refuse permission.[93] Moreover, certain analysis capacities or processing purposes are not foreseeable at the moment of registration. Yet, as scientific progress advances and the network of participating institutions enlarges, the number and variety of possible reuses are enriched.

Solution: A dynamic, just-in-time permission model uses modern communication strategies and technological means to provide the participants with relevant information at the moment when they need to authorise or refuse the collection of data.[94] A dynamic approach enables participants to receive notifications, engage them in the provision of granular authorizations for specific research activities and update their preferences about data access by certain organisations.[95]

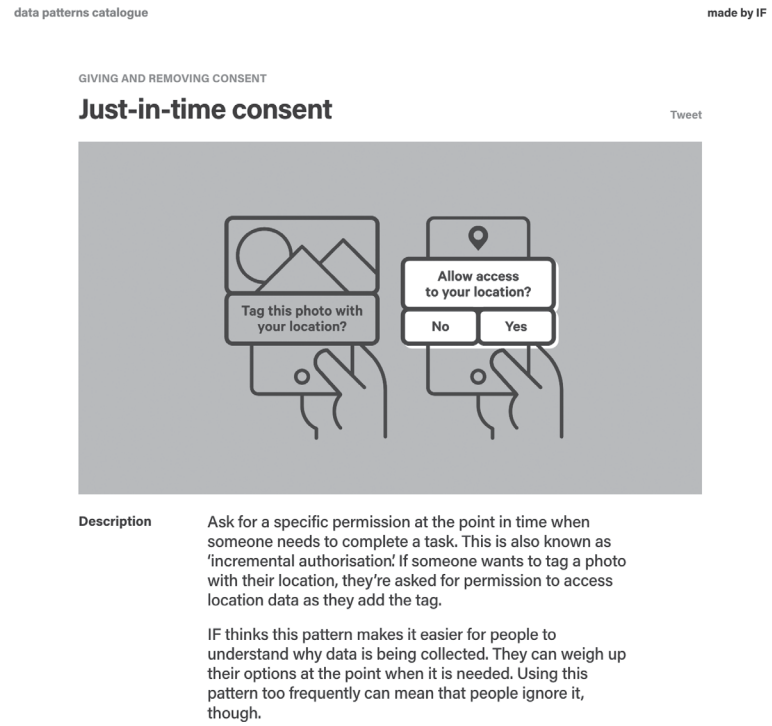

Figure 5.2 Excerpt from IF catalogue of design patterns: just-in-time consent[96]

[93] Sage Bionetworks, 'Just-in-Time Permission' (n 91).

[94] Just-in-time permissions oppose widespread models of broad consent, where participants initially agree to a framework for future research of specific kinds, but are not informed of those unforeseeable or undefined aspects that only emerge as the research unfolds. Due to the incompleteness of information at the moment of decision-making, detractors of this model argue that participants can not be considered informed, therefore broad consent is illegal and unethical. For a discussion, see K Solum Steinsbekk, B Kåre Myskja and B Solberg, 'Broad Consent versus Dynamic Consent in Biobank Research: Is Passive Participation an Ethical Problem?' (2013) 21 *European Journal of Human Genetics* 897.

[95] Budin-Ljøsne and others, 'Dynamic Consent' (2017) 3.

[96] IF, 'Just-in-Time Consent' (Data Patterns Catalogue), available at catalogue.projectsbyif.com/patterns/just-in-time-consent. Licensed under CC BY 4.0: creativecommons.org/licenses/by/4.0.

c. Data Usage Logs[97] and Consent Receipts[98]

Scenario: Imagine an individual who has carefully set dozens of data use permissions. The parties accessing the data must be able to demonstrate compliance with the established permissible use (ie, to demonstrate accountability).

Problem: The expectation that participants memorise or autonomously record their preferences is irrealistic. Moreover, they are unable to check the actual data practices of the other parties and contrast them with the permissions they granted and the declared practices. Without such feedback, participants do not know whether and how the sharing system is functioning, which might cause distrust.

Solution: Data usage logs keep a record of all parties' access to datasets, thereby serving the goal of transparency for all stakeholders involved. It enables participants to receive a tangible return about the helpfulness of their cooperation. This approach can be combined with consent receipts issued as proof of consent for each data use authorised by the participant. The records can be contrasted to find out whether such permissions have been respected or rather breached by certain parties. It is an instrument of transparency for participants and of accountability for organisations processing those records while respecting users' rights.

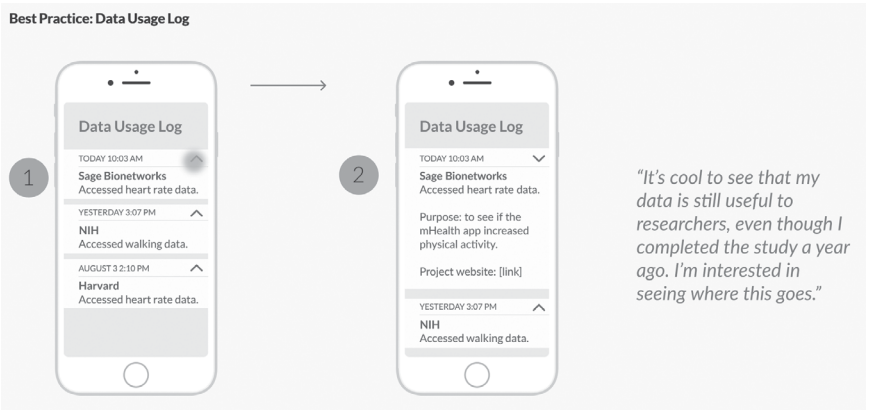

Figure 5.3 Excerpt from SageBionetworks Privacy Toolkit: data usage log interface for biomedical research purposes[99]

[97] Sage Bionetworks, 'Data Usage Log' (Privacy Toolkit), available at designmanual.sagebionetworks.org/data-usage-log.html. See also IF, 'Activity Log' (Data Patterns Catalogue), available at catalogue.projectsbyif.com/patterns/activity-log.

[98] Kantara consent receipt specification, Beaumont, Cooper, D'Agostino, Graves, Henderson, Hodder, Honko, Hughes, Jones, Lapes, Maerz, Maler, Pasquale, Tuoriniemi and Wunderlich, 'Consent Receipt Specification' (2018).

[99] Sage Bionetworks, 'Data Usage Log' (n 97). Used with permission.

V. Conclusion

This chapter has explored the human side of smart contracts, framing them as communicative artefacts that intend to convey information for a purpose. In this context, smart contracts are not just technical or legal tools, but also deeply social tools that impact and are impacted by human behaviour. Our emphasis has been on the application of proactive legal design for the promotion of transparency, autonomy, accountability and trust in the context of health data sharing. This pursuit requires finding a balance between the different stakeholders' often conflicting needs and goals, and embedding transparency into health data sharing services.

We have explored the opportunities that design patterns offer to respond to recurring challenges, so as to translate expectations and values into design-oriented requirements. The user interface layer, when properly designed and built, allows users to translate their intentions into a form that meets their needs, helps them reach their objectives and is legally sound. Our examples illustrate how design patterns offer concrete solutions to increase awareness, engagement and clarity about rights and obligations, with the aim of achieving desirable outcomes and preventing the causes of problems from arising. Although we consider the possible applications to be manifold, we have focused on the design of dynamic informed consent and user-established permissions for information access and use to foster a trustworthy data sharing economy. Future work will explore how proactive legal design can help make, use and humanise smart contracts and promote transparency, trust and compliance in data sharing agreements, security policies and other contexts.