HHAI 2023: Augmenting Human Intellect
P. Lukowicz et al. (Eds.)

doi:10.3233/FAIA230088

Legal-Ethical Challenges and Technological Solutions to e-Health Data Consent in the EU

Xengie DOAN [a,1], Marcu FLOREA [b], and Sarah E. CARTER [c,d]
[a] *SnT, University of Luxembourg*
[b] *University of Groningen, the Netherlands*
[c] *Data Science Institute and the Discipline of Philosophy, University of Galway, Ireland*
[d] *SFI Centre for Research Training in Digitally-Enhanced Reality (D-Real), Ireland*
ORCiD ID: Xengie Doan https://orcid.org/0000-0002-8245-1555, Marcu Florea https://orcid.org/0000-0002-0319-8935, Sarah E. Carter https://orcid.org/0000-0003-3621-5962

Abstract. e-Health data is sensitive and consenting to the collection, processing, and sharing involves compliance with legal requirements, ethical standards, and appropriate digital tools. We explore two legal-ethical challenges: 1) What are the scope and requirements of digital health data consent? 2) What are the legal-ethical reasons for obtaining consent beyond the GDPR's legal basis, and how might such consent be obtained? We then propose human-centered solutions to help navigate standards of ethical and legal consent across the EU, purposefully addressing those use cases to compensate for human difficulties in managing consent without clear guidelines. These solutions – including ISO standards, ontologies, consent mechanisms, value-centered privacy assistants, and layered dynamic consent platforms – complement and aid humans to help uphold ethical and rigorous consent.

Keywords. e-health, dynamic consent, privacy assistants, legal-ethical challenges

1. Introduction

Consent stems from medical consent as an ethical concept (hereafter called "ethical consent") from the 1970s with the principle of respect for autonomy and the dignity of persons. Respect for autonomy is enshrined in ethical guidelines such as the Belmont Report [1] and the Declaration of Helsinki [2]. This understanding of respect for autonomy has been operationalized as *informed consent* [3], which requires that participants in medical research are informed in a sufficiently comprehensive and understandable manner (such as with a notice or information sheet) and that they are not manipulated [4]. Ethics also interacts with the legal dimensions of consent. With a transition to health data sharing using digital technologies (hereafter referred to as "e-health"), a rise in the accessibility of genetic testing, and the advent of AI technologies moving health data away from an

[1] Corresponding Author: Xengie Doan, xengie.doan@uni.lu.

exclusively medical context, ethics' interplay with laws has generated more complexities.

In the European Union (EU), the General Data Protection Regulation (GDPR) sets rather strict conditions for obtaining consent (hereafter referred to as "legal consent") [5]. In addition, health data are considered special under the GDPR because of their sensitivity, requiring more stringent protections and conditions for processing, including explicit consent (Art. 9 GDPR). The GDPR aims to protect the identified or identifiable natural persons whose data is processed ("data subject") by regulating the processing of personal data and reconciling individual control with other rights and interests at stake. However, the rules are difficult to comply with for researchers and companies and exercising rights requires much effort on the part of the data subject who must read, understand, and decide on the processing of their personal data.

Additionally, the newly enacted Data Governance Act (DGA) aims to improve data sharing in the EU by creating a harmonized framework for data exchanges and data governance [6]. The DGA introduces new concepts such as data intermediaries and data cooperatives and regulates the voluntary sharing of data for "altruistic purposes" and the provision of services assisting individuals in giving and withdrawing consent. Thus, the new regulation increases uncertainty regarding how altruism interferes with the GDPR's legal grounds for processing personal data or how data intermediaries or cooperatives will enable individuals to express their privacy choices [7].

As such legal-ethical complexities build in e-health data consent, consent management solutions need to adapt to address the interests of data subjects and data controllers. In particular, such tools should address these interests in a human-centered, responsible manner to maximize human autonomy, promote lawfulness, and increase the transparency of data sharing and associated rights.

In our contribution, we discuss two legal-ethical issues: 1) What are the legal-ethical challenges regarding the scope and requirements for e-health data consent? 2) What are the legal-ethical reasons for obtaining consent beyond its role as a legal basis? Then, we describe available technological solutions and our work in the sphere. Our position is that the implementation of more interoperable, value-centered, and dynamic tools can assist humans in obtaining appropriately ethical and rigorous e-health data consent by helping them navigate legal-ethical uncertainties and challenges.

2. (Un)defined Requirements for Consent

2.1. Upholding Autonomy as an Ethical Principle for Digital Health Data

The rise of e-health data sharing has further muddied ethical debates regarding *how to*, *when to*, and *from whom* to obtain consent in order to uphold autonomy. While paper-based consent was debated in terms of understandability and transparency, data-collecting digital medicine devices add unique challenges. They contain often long and jargon-filled user agreements and introduce a layer of consent between company and patient [8]. For example, some smartphone mobile health ("mHealth") apps allow health data traditionally reserved for the doctor and patient to be accessible for other commercial purposes, such as third-party marketing [9]. Apps may also lack privacy policies and terms of agreements altogether, and if present, are difficult to read and comprehend [10].

Unlike more rigid consent practices in medicine, this data is given with a click of a privacy permission request on a smartphone, often with little understanding of what is being given away [11]. From an ethical perspective, this raises concerns about how informed an individual's consent is and skepticism that it upholds the principle of autonomy.

2.2. *Who is the Genetic Data Subject?*

Health data is sensitive due to the interconnected nature of the data. Here, we focus on a highly connected and identifiable subset of e-health data, genomic data. With millions sequencing their DNA due to increased accessibility [12], distributed privacy risks have become even greater [13,14]. While there are varying guidelines across countries for giving notice to family members that their shared genetic data is being processed [15], from an ethical perspective, Minari et al. [16] argues for a form of family-group consent for genetic data processing because of shared risks.

Legally, a genetic group as a data subject is considered in guidelines but enforcement is unclear. The European Data Protection Board (EDPB) guidelines on genetic data state that data subjects can be families [17]. However, individual and collective enforcement under the GDPR is complex [18] due to the possibility of conflicting rights, such as the right to object to processing from one individual [19], the *right not to know* [20,21], or the right to process their data. There is little existing guidance on how to resolve such conflicts and is an area of active debate [22,19]. It has been argued that managing conflicts is feasible [23] with the GDPR as a starting point. In addition, different countries have various approaches to weighing the rights of all parties based on the context and existing rulings (e.g. the right to privacy of the deceased is overruled by the right to health of the living [24]) and laws. This may also help data minimization principles by limiting data sharing and access to only well-justified cases [23]. While ethical and legal guidelines may allow for a collective interpretation, this challenges the status quo of individual consent and further complicates GDPR enforcement.

2.3. *Specificity in Consent: Purposes and Controllers*

While consent must be "*specific, informed, and freely given*" (Art. (4)(11) GDPR), guidelines around purpose specificity from a legal-ethical perspective are unclear or contradictory. First, specificity is arguably at odds with broad consent models used in biomedical research. Broad consent refers to consent for specific and general future purposes, while specific consent refers to consent for an explicit purpose. From an ethical perspective, broad consent could be acceptable if the individual is provided sufficient knowledge to be informed [4] – although whether current e-health consent meets these criteria and upholds autonomy is debatable. Second, though data protection law mandates specific consent, issues regarding interpretation remain. For example, too narrow an interpretation of specificity may lead to frequent re-consent from data subjects and induce consent fatigue [25]. Also, Recital 33 GDPR acknowledges that it is often impossible to identify all purposes of personal data processing for scientific research at the time of data collection and offers a solution of consent for "*certain areas of scientific research when in keeping with recognized ethical standards*". However, this is not reflected in the text of the GDPR itself, which advocates for specificity, and is open to different interpretations of scope and application [26,27,28].

For consent to be valid, the data subject should also be given the identity of the entity that decides on the means and purpose of the processing ("data controller") (Recital 42 GDPR). However, this can be difficult to identify at the time of initial collection and the text of the GDPR is not clear on the elements that must be provided. While Article 13(1)(a) GDPR and Recital 42 GDPR require that the identity of the data controller to be disclosed, Article 13(1)(e) suggests that the entities that process personal data can be clustered based on relevant criteria by referring to information about recipients or "categories of recipients". The notion of "recipient" (Art. 4(9) GDPR) can include third parties, but also controllers and processors, rendering the contents for the obligation to inform uncertain. The new DGA [6] further complicates the recipient's identity. In complex data-sharing environments, it is unclear whether re-consent should be asked when additional persons become involved in the data processing. Such persons include those who process personal data on behalf of the data controller ("data processors"), additional data controllers, or new third parties that become involved after initial consent.

In summary, the debates about how to uphold autonomy as an ethical principle, if a genetic data subject under the GDPR can be collective, and how specific consent is regarding purposes and the data controllers all lack guidelines for e-health consent.

3. Consent is Relevant, Even When Not the Legal Basis

Even when consent is not the legal basis for processing data (Art. 6(1)(c)-(f) GDPR), such as legitimate interest, or the data falls under an exception for processing health data (Art. 9(2)(i)(j) GDPR), such as public health, ethical consent is relevant due to the possible legal consequences as an ethical standard or safeguard. Such data processing is subject to a balancing exercise based on the proportionality of interests and rights of the data subject and processor, which often requires the implementation of safeguards to help protect rights. Recital 33 of the GDPR refers to "*recognized ethical standards*" but lacks details or references. Then, Art. 9(2)(j) GDPR provides that health data can be processed for scientific research purposes based on Union or Member State law provided that appropriate safeguards are in place. Next, Article 89 of the GDPR also requires safeguards when data is processed for research purposes, but again the text lacks any definitions. In another instrument in the EU [29] or outside the EU [20,2,30], consent is a condition for participation in biomedical research. Commenting on the safeguards in the GDPR, Staunton et. al. [31] argues that ethical requirements such as consent and transparency could serve as safeguards to help inform the data subject of their rights.

The distinction between consent for research and consent for processing personal data must also be clearly communicated, and possibly combined through consent management platforms (CMPs). The EDPB [32] differentiates between the functions wherein *consent for participation in research* protects human dignity and the right to integrity of individuals while *consent for processing of personal data* is a requirement connected to the right to protection of personal data. The European Data Protection Supervisor (EDPS) also notes this separation and argues that informed consent can function as a safeguard for data subject rights' in medical research [27]. The Commission DG Research & Innovation Guidance suggests that consent for lawfully processing personal data and informed consent for research could be integrated with CMPs to increase transparency to the data subject when it is difficult to identify the purpose of the research [33]. While

CMPs can more transparently communicate processes and rights to data subjects, they can also confuse data subjects. If individuals provide their informed consent to participation in biomedical research, it might come as a surprise that the ground for processing personal data is not consent. If the distinction is not made clear, it might give the false impression that the data subject is in control. For example, the data subjects do not have the right to withdraw consent (Art. 7(3) GDPR) or the right to data portability (Art. 20 GDPR) when consent is not the legal basis for processing data. Therefore, consent as a safeguard should be clearly explained to data subjects and differentiated from consent as a legal basis. Overall, it remains unclear whether the proposed CMPs would comply with the current requirements of legal consent or act as a legal safeguard, and if this could extend to cases for general health data sharing and not only for biomedical research.

From an ethical standpoint, one can argue that ethical consent in e-health should always be part of health data collection to uphold autonomy. The Belmont Report argues for respect for autonomy as a critical component of upholding human dignity through Principlism [34]. However, autonomy and ethical consent have been critiqued by bioethicist Onora O'Neill [35] who argued that this interpretation diminishes trust, wherein doctors value legal compliance more than true empathetic communication. It has also been critiqued for undervaluing collective concerns in favor of individual considerations. For example, one individual's consent to sharing genetic data may implicate genetic relatives without their knowledge through data breaches [36], yet despite these shared risks, only one individual consented. Despite these concerns about the Belmont Report's operationalization of autonomy into individual informed consent, few would argue that respect for autonomy is not worth upholding — but it may require a different ethical justification. Respect for autonomy can also be rooted in Flourishing Ethics (FE) [37,38], which proposes that the pursuit and promotion of human flourishing is the ultimate ethical "good." FE brings together a group of related understandings in computer and information ethics that have this idea of human flourishing as their primary ethical concern [39,40,41,42]. In FE, "autonomy" is viewed as a requirement for human beings to flourish [38]. In psychology, theories exploring psychological well-being such as self-determination theory (SDT) translate philosophical understandings of human flourishing and autonomy [43]. SDT postulates that designing autonomous digital interactions requires interfaces or assistive technologies to promote both a user's sense of agency and consistency with a user's values, goals, and sense of purpose [44,43]. In the case of health data, notice and consent (though flawed) allow an exercise of autonomy on the flow of their data to shape an increasingly important aspect of modern life: one's digital footprint. Forgoing this control, or coercing it, could undermine human flourishing [41].

4. Technological Solutions to Ethical-Legal Challenges

In this section, we identify and discuss technological solutions that we believe can help tackle the above ethical-legal challenges in e-health consent. We provide a critical analysis of existing solutions and our work towards more dynamic, transparent, and value-centered consent. These solutions center collaborations between technology and humans (data controllers, processors, subjects) to promote agency and value-centered choices.

4.1. Technical Standards, Ontologies, and Mechanisms for Consent

To address the lack of guidelines for specific consent and purpose specification in Sec. 2.3, we look towards technical standards from the International Organization for Standardization (ISO) and ontologies built by expert communities. To address the role of consent even when it is not the legal basis from Sec. 3, consent mechanisms with options to object to data processing by legitimate interest will be analyzed.

First, ISO/IEC 29184 describes the structure and content of online consent and privacy notices to collect and process personally identifiable individual data. It outlines how to communicate transparent and understandable information about the data collection and processing, as well as how to obtain consent to be "*fair, demonstrable, transparent, unambiguous and revocable*" [45]. It has also been shown to enable compliance with the GDPR [46] and could be compatible with the DGA, which requires the development of an altruistic consent form at the EU level available in an electronic, machine-readable form using a modular, customizable approach for specific sectors and purposes (Art. 22 DGA). However, as a closed standard with licensing fees, adoption by individuals or institutions with fewer resources may be difficult.

Second, the ISO standard suggests using consent policies based on standardized semantic vocabularies, such as the World Wide Web Consortium's (W3C's) Data Privacy Vocabulary (DPV) [47], which can also aid in the specificity of consent. The semantic web is an effort from W3C to make the internet machine-readable and enable a web of linked data with vocabularies, query languages, and more. The DPV is an ontology about the use and processing of personal data with terms including processing purposes. Ontologies can be extended for different use cases (e.g., a GDPR compliant extension of the DPV [48]) or mapped to other compliant ontologies [49,50]. They could also create "parts of research projects" to offer categories instead of single choices (Recital 33 GDPR). As an open-source technology, organizations can contribute and help address their use cases or map the logic of DPV to other ontologies. For example, terms in the DPV can be mapped with concepts in the Data Use Ontology (DUO) [51]. Created by the Global Alliance for Genomics and Health, DUO addresses data sharing after consent and increases the FAIRness (ability to be findable, accessible, interoperable, and reusable) [52]. Other health ontologies [53,54,55] could be mapped and connected to standardize consent, data sharing, e-health records, and other health processes. While more work is required to make ontologies such as DPV applicable to more health data-sharing situations, we can envision an interoperable future for privacy, consent, data sharing, and legal compliance based on extensive open vocabularies. This can also help automate the activity of data intermediaries or cooperatives regulated under the DGA.

Third, these standards and ontologies can be communicated through the web using Data Protection and Consenting Communication Mechanisms (DPCCMs), containing the "*communication of data, metadata, information, preferences, or/and decisions related to data protection or/and consenting between different actors*" that can be used on the web or apps [56]. Examples include Do Not Track or Advanced Data Protection Control (ADPC). ADPC is more complex than a binary track or do not track, and can express the specific purpose along with the consent decision and object to processing based on legitimate interest. These technologies could also have a role in compliance with data protection law as it offers a way to object to processing when consent is not the legal ground for processing. Furthermore, ADPC could incorporate more complex values such

as consent preferences, thereby enabling personalization across platforms using ADPC. However, some challenges still remain. There is no standardized process for developing the vocabularies regarding the values in ADPC, and adoption of such DPCCMs remains challenging, as with the obsolescence of Platform for Privacy Preferences Project (P3P) [57]. DPCCMs could contribute to a more central ecosystem of consent to facilitate purpose specification, processing entities, and privacy profiles. While ADPC could enable increased autonomy through the ability to object to processing when the legal basis is legitimate interest, the rights could still be obscured if the consent mechanism is not widely adopted. Similarly, while guidelines for specific consent are part of ISO standards and ontologies can increase specificity, a more unified and interoperable consent ecosystem requires social factors to gain traction outside the scope of this paper.

4.2. Ethical and User-Friendly Privacy Assistants

We can also consider technological assistants to better promote autonomy, value-centered choices, and human flourishing in smartphone mHealth settings (Secs. 2.1 and 3). When apps are collecting health data, personalized privacy assistants (PPAs) could help empower humans to navigate consent permissions and promote more autonomous action. Smartphone PPAs use a decision tree to ask the user a series of privacy preference questions and determine their privacy preference profile. From this profile, PPAs provide the user with privacy setting notifications and privacy setting recommendations for the apps on their phone [58]. For users who use mHealth apps, such recommendations could remind them of their privacy preferences when they may have "clicked through" permission settings when downloading the app. Infrastructure for PPAs for the Internet of Things (IoT) has also been proposed, and such a system could help users manage data collected by complex, multi-system health sensors or medical devices by giving them similar notifications and recommendations [59].

A related system under development is the value-centered privacy assistant (VcPA) [60], which aims to promote value-centered choices at the root of human wellbeing and flourishing [44,43]. Profiles are based on how a user's personal values are involved in their app selection and privacy decision-making by mapping values onto acceptable data collection practices [61]. Notifications occur before downloading an app from the app store. These notifications serve as "selective friction" to warn users when they may be downloading an app that conflicts with their value set as determined by their profile. It also recommends alternative applications with similar functions that are more consistent with a user's values.

Both systems encourage users to exercise their autonomy when engaging with mHealth apps by assisting them with data privacy decisions that they may otherwise quickly click through or struggle to comprehend the privacy policies and terms of agreement [10,11]. This more judicious use of collaborative technologies, by promoting autonomy, furthers human well-being and flourishing in the e-health data space [43].

4.3. Layered User-centered Dynamic Consent

Last, dynamic consent (DC) can incorporate the above technologies, enable autonomy, and increase specificity of consent regarding the genetic data subject (individual and collective), data processing purposes, and processing entities in Sec. 2. DC is a model

of consent and digital platform centering data subjects in facilitating consent over time [62,63,64]. DC can request specific consent over time as data processing or the controller changes and be layered in terms of the type of consent (specific or broad) or information, allowing users to choose the depth of information and type of consent they prefer. On such systems, perhaps specific consent could be the default, with a layered approach that first shows key information and then offers more detailed information with broad consent as a secondary option. It could be personalized based on the data controller and data subject's legal jurisdiction, privacy preferences, and values – with value–centered privacy assistants to help make decisions. Similarly, collective specific consent could be a default for genetic data sharing unless the individual chooses broad consent, and in the case of conflicting rights specific and granular rights can be carried out and relayed to the data collector to resolve issues more transparently.

As a platform, DC can also incorporate ISO standards, consent ontologies, and shared consent mechanisms. If multiple DC platforms use interoperable ontologies and/or consent mechanisms, a more unified consent management system could be envisioned. However, work from the technological side is needed to suit more use cases and larger societal challenges stand in the way of adopting shared technologies. To this end, Author 1 is working to identify and validate non-functional requirements for collective DC and propose an interoperable and transparent model of collective DC based. This work is based on research on consent which theorizes on collective DC but lacks technical proposals [65,16] and a user study regarding key elements of consent [66]. Author 2 is working on the role of a DC model in compliance with GDPR and the DGA to improve transparency and safeguard the interests of the data subjects while enabling the free flow of personal data in a biomedical context. Author 3 is exploring how our values are involved in our smartphone data privacy decisions in order to best design, deploy, and time privacy notices based on values. The initial conceptual groundwork has been laid and the aforementioned VcPA is under development [60,61]. A forthcoming paper will identify points of improvement for the VcPA in order to best assist users in making a privacy decision consistent with their privacy preferences and values.

5. Conclusion

Technology can work to manage ethical-legal consent challenges for e-health data, especially when human needs are centered and not legal-ethical compliance. We build on consent standards, ontologies, and mechanisms, privacy assistants working with users' values to manage consent decisions, and propose layered (collective and/or individual) dynamic consent to enhance autonomy and specificity. Some technologies still require further development to truly address the challenges, and the authors are researching legal, ethical, and technical aspects in their future work. From this, the wider adoption of these solutions could not only tackle ongoing legal-ethical ambiguity within the EU but also lay the foundation for cross-border health data transfers between different countries. Despite differing guidelines and requirements, a united technological front and deployment of human-centered tools for e-health management could help provide the basis for greater communication, understanding, and harmonization between jurisdictions.

Acknowledgments. This work is financially supported by EU H2020 projects LeADS (Grant ID:956562) and KnowGraphs (Grant ID:860801) and SFI CRT d-real (Grant No. 18/CRT/6224). We also thank Cost EU PIDSKG Workshop CA19134.

References

[1] Ryan KJ, Brady JV, Cooke RE, Height DI, Jonsen AR, King P, et al. The Belmont Report. Washington D.C.: US Department of Health, Education, and Welfare; 1979.

[2] World Medical Association. Declaration of Helsinki, ethical principles for scientific requirements and research protocols; 2013. 4.

[3] Beauchamp TL. Informed consent: its history, meaning, and present challenges. Cambridge Quarterly of Healthcare Ethics. 2011;20(4):515-23.

[4] Childress JF. The Place of Autonomy in Bioethics. The Hastings Center Report. 1990;20(1):12-7.

[5] Regulation (EU) 2016/679 (General Data Protection Regulation). vol. 119; 2016. Available from: http://data.europa.eu/eli/reg/2016/679/oj/eng.

[6] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act); 2022. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767.

[7] Solove DJ. Introduction: Privacy self-management and the consent dilemma. Harv L Rev. 2012;126:1880.

[8] Klugman CM, Dunn LB, Schwartz J, Cohen IG. The Ethics of Smart Pills and Self-Acting Devices: Autonomy, Truth-Telling, and Trust at the Dawn of Digital Medicine. American Journal of Bioethics. 2018;18(9):38-47. Available from: https://doi.org/10.1080/15265161.2018.1498933.

[9] Lucivero F, Jongsma KR. A mobile revolution for healthcare? Setting the agenda for bioethics. Journal of Medical Ethics. 2018;44(10):685-9.

[10] Robillard JM, Feng TL, Sporn AB, Lai JA, Lo C, Ta M, et al. Availability, readability, and content of privacy policies and terms of agreements of mental health apps. Internet interventions. 2019;17:100243.

[11] Kelley PG, Cranor LF, Sadeh N. Privacy as part of the app decision-making process. In: Bødker S, Brewster S, Baudisch P, Beaudouin-Lafon M, Mackay WE, editors. Proceedings of the Conference on Human Factors in Computing Systems (CHI). Paris: ACM; 2013. p. 3393-402.

[12] Mardis ER. A decade's perspective on DNA sequencing technology. Nature. 2011;470(7333):198-203.

[13] Bonomi L, Huang Y, Ohno-Machado L. Privacy challenges and research opportunities for genomic data sharing. Nature genetics. 2020;52(7):646-54.

[14] Erlich Y, Shor T, Pe'er I, Carmi S. Identity inference of genomic data using long-range familial searches. Science. 2018;362(6415):690-4.

[15] Takashima K, Maru Y, Mori S, Mano H, Noda T, Muto K. Ethical concerns on sharing genomic data including patients' family members. BMC Medical Ethics. 2018 Jun;19(1):61.

[16] Minari J, Teare H, Mitchell C, Kaye J, Kato K. The emerging need for family-centric initiatives for obtaining consent in personal genome research. Genome Medicine. 2014 Dec;6(12):118.

[17] 12178/03/EN WP 91 Working Document on Genetic Data; 2004. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf.

[18] Kuru T. Genetic data: The Achilles' heel of the GDPR? Eur Data Prot L Rev. 2021;7:45.

[19] Kuru T, de Miguel Beriain I. Your genetic data is my genetic data: Unveiling another enforcement issue of the GDPR. Computer Law & Security Review. 2022;47:105752.

[20] of Europe C. Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine; 1997. Available from: https://rm.coe.int/168007cf98.

[21] UNESCO. Universal Declaration on the Human Genome and Human Rights;. Available from: https://www.unesco.org/en/legal-affairs/universal-declaration-human-genome-and-human-rights.

[22] Knoppers BM, Kekesi-Lafrance K. The Genetic Family as Patient? American Journal of Bioethics. 2020 Jun;20(6):77–80.

[23] Beriain IDM, Jove D. Is it possible to place limits on the self-determination of your own genetic data? Certainly, and there is an urgent need for it! BioLaw Journal-Rivista di BioDiritto. 2021;(1S):209-22.

[24] per la Protezione dei Dati Personali G. Dati inerenti allo stato di salute - dati genetici, Cittadini e socie-tà dell'informazione; 1999. Available from: https://www.garanteprivacy.it/documents/10160/10704/996886.

[25] Choi H, Park J, Jung Y. The role of privacy fatigue in online privacy behavior. Computers in Human Behavior. 2018;81:42-51.

[26] for German Supervisory Authorities A. Guidance on the interplay between recital 33 and the definition of consent in the GDPR; 2019. Available from: https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf.
[27] Supervisor EDP. Preliminary Opinion on data protection and scientific research; 2023. Available from: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en.
[28] Hallinan D. Broad consent under the GDPR: an optimistic perspective on a bright future. Life Sciences, Society and Policy. 2020 Jan;16(1):1. Available from: https://doi.org/10.1186/s40504-019-0096-3.
[29] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. vol. 158; 2014. Available from: http://data.europa.eu/eli/reg/2014/536/oj/eng.
[30] Assembly WG. WMA Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks; 2016. Available from: https://www.wma.net/what-we-do/medical-ethics/declaration-of-taipei/.
[31] Staunton C, Slokenberga S, Mascalzoni D. The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. European Journal of Human Genetics. 2019 Aug;27(8):1159-67. Number: 8 Publisher: Nature Publishing Group. Available from: https://www.nature.com/articles/s41431-019-0386-5.
[32] Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) | European Data Protection Board; 2019. Available from: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en.
[33] European Commission DG Research & Innovation. Ethics and data protection; 2021. Available from: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf.
[34] Beauchamp TL, Rauprich O. Principlism. In: ten Have H, editor. Encyclopedia of Global Bioethics. Champlain: Springer; 2016. p. 1-12.
[35] O'Neill O. Autonomy and Trust in Bioethics. Cambridge: Cambridge University Press; 2002. Available from: https://www.cambridge.org/core/product/identifier/9780511606250/type/book.
[36] NortonLifeLock. MyHeritage data breach exposes info of more than 92 million users; 2018. Available from: https://us.norton.com/blog/emerging-threats/myheritage-data-breach-exposes-info-of-more-than-92-million-user.
[37] Bynum TW. The foundation of computer ethics. Computers and Society. 2000;30(2):6-13.
[38] Bynum TW. Flourishing ethics. Ethics and Information Technology. 2006;8(4):157-73.
[39] Kantar N, Bynum TW. Global ethics for the digital age – flourishing ethics. Journal of Information, Communication and Ethics in Society. 2021;19(3):329-44.
[40] Wiener N. The Human Use of Human Beings: Cybernetics and Society. 2nd ed. Houghton Mifflin; 1950.
[41] Moor JH. Just consequentialism and computing. Ethics and Information Technology. 1999;1(1):65-9.
[42] Floridi L. Information ethics: On the philosophical foundation of computer ethics. Computer Ethics. 1999;1:37-56.
[43] Ryan RM, Curren RR, Deci EL. What humans need: Flourishing in Aristotelian philosophy and self-determination theory. In: Waterman AS, editor. The Best within Us: Positive Psychology Perspectives on Eudaimonia. American Psychological Association; 2013. p. 57-75.
[44] Peters D, Calvo RA, Ryan RM. Designing for motivation, engagement and wellbeing in digital experience. Frontiers in Psychology. 2018;9.
[45] for Standardization IO. ISO/IEC 29184:2020; 2020. Available from: https://www.iso.org/standard/70331.html.
[46] Pandit HJ, Krog GP. Comparison of notice requirements for consent between ISO/IEC 29184: 2020 and General Data Protection Regulation. Journal of Data Protection & Privacy. 2021;4(2):193-204.
[47] Pandit HJ. Data Privacy Vocabulary ({{DPV}}): Concepts for Legal Compliance; 2022.
[48] Ryan P, Pandit HJ, Brennan R. In: A Common Semantic Model of the GDPR Register of Processing Activities; 2020. ArXiv:2102.00980 [cs]. Available from: http://arxiv.org/abs/2102.00980.
[49] Debruyne C, Riggio J, De Troyer O, O'Sullivan D. An Ontology for Representing and Annotating

Data Flows to Facilitate Compliance Verification. In: 2019 13th International Conference on Research Challenges in Information Science (RCIS). IEEE; 2019. p. 1-6.

[50] Palmirani M, Martoni M, Rossi A, Bartolini C, Robaldo L. Legal ontology for modelling GDPR concepts and norms. In: Legal Knowledge and Information Systems. IOS Press; 2018. p. 91-100.

[51] Pandit HJ, Esteves B. Enhancing Data Use Ontology (DUO) for Health-Data Sharing by Extending it with ODRL and DPV;. Preprint on webpage at https://www.semantic-web-journal.net/system/files/swj3127.pdf.

[52] Lawson J, Cabili MN, Kerry G, Boughtwood T, Thorogood A, Alper P, et al. The Data Use Ontology to streamline responsible access to human biomedical datasets. Cell Genomics. 2021;1(2):100028.

[53] Vajda J, Otte JN, Stansbury C, Manion FJ, Umberfield E, He Y, et al. Coordinated evolution of ontologies of informed consent. ICBO. 2018.

[54] Dolin RH, Alschuler L, Beebe C, Biron PV, Boyer SL, Essin D, et al. The HL7 clinical document architecture. Journal of the American Medical Informatics Association. 2001;8(6):552-69.

[55] Kalra D, Beale T, Heard S. The openEHR foundation. Studies in health technology and informatics. 2005;115:153-73.

[56] Human S, Pandit HJ, Morel V, Santos C, Degeling M, Rossi A, et al. Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges. In: 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE; 2022. p. 231-9.

[57] Schwartz A. Looking back at P3P: lessons for the future. Center for Democracy & Technology. 2009.

[58] Liu B, Andersen MS, Schaub F, Almuhimedi H, Zhang S, Sadeh N, et al. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In: Zurko ME, Consolvo S, Smith M, editors. Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS). Denver: USENIX; 2016. p. 27-41.

[59] Das A, Degeling M, Smullen D, Sadeh N. Personalized privacy assistants for the internet of things: Providing users with notice and choice. IEEE Pervasive Computing. 2018;17(3):35-46.

[60] Carter SE. A Value-Centered Exploration of Data Privacy and Personalized Privacy Assistants. Digital Society. 2022;1(27):1-24. Available from: https://doi.org/10.1007/s44206-022-00028-w.

[61] Carter SE, Tiddi I, Spagnuelo D. A "Mock App Store" Interface for Virtual Privacy Assistants. In: Schlobach S, Pérez-Ortiz M, Tielman M, editors. HHAI2022: Augmenting Human Intellect: Proceedings of the First International Conference on Hybrid Human-Artificial Intelligence. IOS Press; 2022. p. 266-8. Available from: 978-1-64368-309-6.

[62] Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: a patient interface for twenty-first century research networks. European journal of human genetics. 2015;23(2):141-6.

[63] Haas MA, Teare H, Prictor M, Ceregra G, Vidgen ME, Bunker D, et al. 'CTRL': an online, Dynamic Consent and participant engagement platform working towards solving the complexities of consent in genomic research. European Journal of Human Genetics. 2021;29(4):687-98.

[64] Mascalzoni D, Melotti R, Pattaro C, Pramstaller PP, Gögele M, De Grandi A, et al. Ten years of dynamic consent in the CHRIS study: informed consent as a dynamic process. European Journal of Human Genetics. 2022;30(12):1391-7.

[65] Prictor M, Huebner S, Teare HJ, Burchill L, Kaye J. Australian Aboriginal and Torres Strait Islander collections of genetic heritage: the legal, ethical and practical considerations of a dynamic consent approach to decision making. Journal of Law, Medicine & Ethics. 2020;48(1):205-17.

[66] Doan XC, Selzer A, Rossi A, Botes WM, Lenzini G. Conciseness, interest, and unexpectedness: User attitudes towards infographic and comic consent mediums. In: Web Conference Companion Volume (ACM). ACM; 2022. .