Article | Received 11 February 2026; Revised 16 June 2026; Accepted 1 July 2026; Published X August 2026
https://doi.org/10.55092/let20260013

Reconstructing consent in genomic AI: SCOT, respect for persons, and the case for dynamic consent

Nabila khwaja*, Amal Robay

Department of Research, Weill Cornell Medicine, Doha, Qatar

* Correspondence author; E-mail: Nwk4001@Qatar-med.cornell.edu.

Highlights:

- Applies SCOT and PRP to demonstrate how regulatory categories such as broad consent, minimal risk, and compatible purpose are socially constructed, institutionally stabilised, and ethically consequential.
- Demonstrates why static consent and categorical exemptions under the U.S. Common Rule are inadequate for the evolving, cumulative, and intergenerational risks that characterise AI-driven genomic research.
- Reconceptualises informed consent in genomic AI as a dynamic, relational process grounded in GDPR Articles 5, 6(4), 9(2)(a)/(j), and 89(1), with Recital 33 guiding interpretation but neither authorising processing nor constituting an independent legal basis for research processing.
- Argues that dynamic consent is not an independent lawful basis under the GDPR but may offer a doctrinally compatible and ethically robust governance mechanism capable of operationalising existing obligations under Articles 5, 6, 9, 12–14, and 89(1), thereby enabling iterative engagement, granular permissions, and accountability across evolving research contexts, particularly in dual-regulation environments such as Qatar, where GDPR-style frameworks coexist with U.S. Common Rule requirements.

Abstract: Artificial intelligence (AI)-driven genomic research challenges prevailing consent frameworks by enabling iterative data reuse, cumulative inference, and intergenerational risk that static, one-off consent cannot adequately address. This article applies the Social Construction of Technology (SCOT) and the principle of Respect for Persons (PRP), interpreted through relational autonomy, to examine how regulatory categories such as broad consent, minimal risk, and compatible purpose are socially constructed, institutionally stabilised, and ethically consequential. In this context, consent rules operate not merely as mechanisms of authorisation but as governance tools that allocate responsibility, shape expectations, and determine the legitimacy of downstream data use over time. Through a comparative analysis of the EU General Data Protection Regulation (GDPR) and the U.S. Common Rule (U.S.C.R.), the article demonstrates how categorical exemptions and procedural consent under the U.S.C.R. fail to ensure sustained participant protection in genomic AI, while the GDPR embeds consent within a cumulative legality architecture grounded in Articles 5, 6(4), 9, and 89(1), with Recital 33 guiding interpretation. The article argues that dynamic consent does not constitute an independent lawful

basis under the GDPR but may offer a doctrinally compatible and ethically robust governance mechanism capable of operationalising existing GDPR obligations. It may do so by enabling iterative engagement, granular permissions, and accountability across evolving research contexts, particularly in dual-regulation environments such as Qatar, where GDPR-style frameworks coexist with U.S.C.R. requirements.

Keywords: dynamic consent; relational autonomy; genomic AI; GDPR Article 9; Recital 33; Social Construction of Technology (SCOT); Respect for Persons; Common Rule; exemption frameworks; data ethics

1. Introduction

Artificial intelligence (AI) is reshaping genomic research through real-time analysis, predictive modelling, and adaptive data use across clinical and public health contexts. However, static, one-off consent and categorical exemptions cannot accommodate AI's evolving and cumulative risks. A relational conception of autonomy exposes these gaps by situating consent within social, familial, and institutional contexts [1,2]. Genomic surveillance further intensifies concerns about consent, re-identifiability, and the erosion of purpose limitation through model reuse [3,4]. These challenges are amplified by the integration of AI analytics [5]. This is particularly evident where real-time surveillance relies on large-scale integration of clinical, genomic, and epidemiological data. AI exposes the limits of traditional consent and categorical exemptions [6]. Ethnographic studies show that data-science practices evolve continuously, rendering static consent and fixed risk thresholds inadequate for iterative, AI-mediated reuse [7,8]. Consent rules in this context perform multiple, socio-legally significant functions: they do not merely authorise data processing, but structure expectations, allocate responsibility between actors, and define the conditions under which data may be legitimately reused over time.

This governance function operates across three distinct settings that this article examines in turn. In clinical settings, genomic data collected for diagnostic purposes are routinely repurposed for AI model training. The DeepMind–Royal Free National Health Service (NHS) arrangement illustrates this concretely: patient records collected for direct care were transferred for AI development without adequate patient notification, triggering findings of unlawful processing under the General Data Protection Regulation's (GDPR's) compatibility and transparency requirements. In commercial settings, direct-to-consumer genomic platforms such as 23andMe have used one-off consent to authorise data licensing, internal research, and commercial partnerships. Downstream uses proceeded without compatibility assessment or renewed participant engagement. These outcomes reflect the structural gaps in the U.S. Common Rule's (U.S.C.R.'s) requirements exemption-based architecture. In dual-regulation environments such as Qatar, studies simultaneously fall under GDPR-inspired data protection frameworks and U.S.C.R. requirements triggered by federal funding. Institutions must navigate divergent consent standards without coherent cross-jurisdictional governance. Transparency and accountability are therefore not incidental aspirations but structural conditions of lawful and ethical data governance across each of these settings.

Comparing the General Data Protection Regulation (EU) 2016/679 (GDPR) and the U.S. Common Rule 2018 (U.S.C.R.) is essential because these regimes dominate biomedical research governance and exert global influence. The GDPR's extraterritorial reach shapes EU Gulf Cooperation Council (GCC) data flows, while U.S. funding frequently triggers U.S.C.R. oversight, making their divergent treatment of autonomy

and consent directly consequential for institutions operating across both frameworks. Although both frameworks aim to protect research participants, they diverge fundamentally in their treatment of autonomy. Genomic AI exposes this divergence, as categorical exemptions under the U.S.C.R. prioritise procedural closure over ongoing oversight, failing to track downstream reuse or sustain participant understanding across evolving research contexts [9]. To address this, we apply two complementary lenses: the Social Construction of Technology (SCOT), which shows how categories such as 'consent' and 'minimal risk' are socially negotiated and stabilised, and the principle of Respect for Persons (PRP), extended through relational autonomy, which reframes consent as an ongoing ethical relationship rather than a one-off transaction. These conceptual anchors, elaborated in Boxes 1 and 2, provide the framework for our comparative analysis of the GDPR and the U.S.C.R. in genomic AI. These governance tensions are illustrated in Figure 1, which identifies structural 'cracks' in consent across regulatory frameworks, and Figures 2, which outlines how these gaps may be addressed through governance mechanisms capable of sustaining transparency, accountability, and participant engagement over time.

Box 1. The Social Construction of Technology

The SCOT, developed by Pinch and Bijker (1984), frames technologies not as fixed artefacts but as socially constructed outcomes shaped by "interpretive flexibility." Artefacts and legal categories such as "consent," "risk," or "exemption" gain meaning through negotiation among relevant social groups (engineers, regulators, researchers, participants) Stabilisation occurs when one interpretation becomes dominant, often privileging efficiency or institutional convenience. In governance, this means that apparently neutral categories embed social values, compromises, and power dynamics rather than objective truths.

Box 2. Respect for Persons and relational autonomy

The PRP, canonically formulated in the Belmont Report (1979) and by Beauchamp & Childress (2019), holds that individuals must be treated as ends in themselves, never merely as means. It grounds research ethics in two requirements: respect for autonomy and additional protections for those with diminished or constrained autonomy. Contemporary feminist scholarship extends this to "relational autonomy," recognising that autonomy is socially embedded, institutionally mediated, and shaped by family and community ties (Mackenzie & Stoljar 2000). In genomic AI, this requires that consent be iterative and relational an ongoing ethical relationship rather than a one-time transaction.

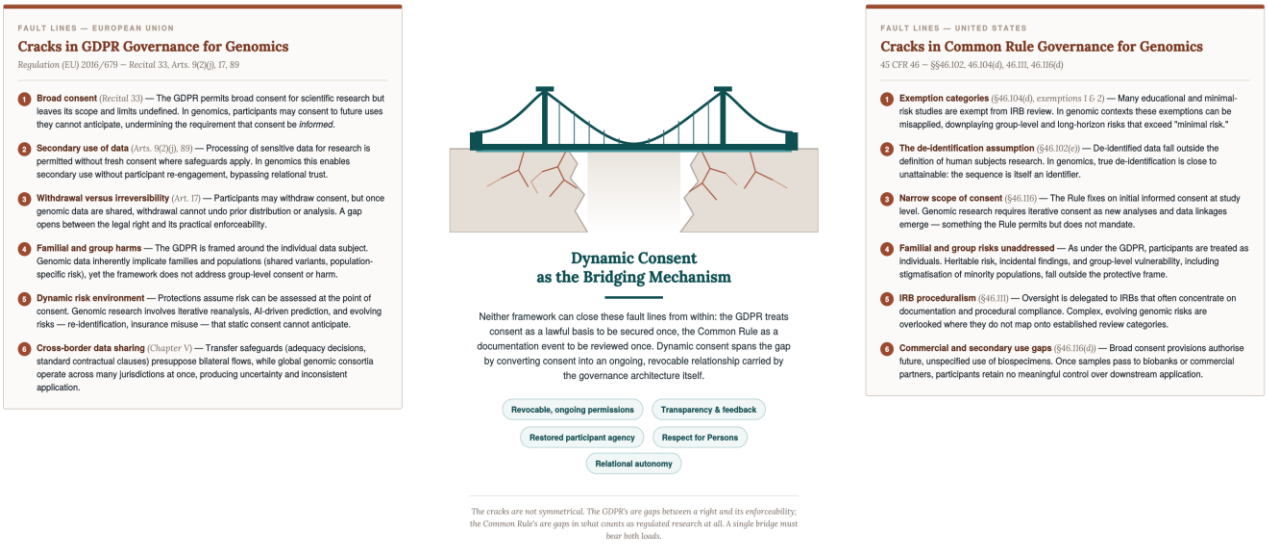

Figure 1. Cracks in the consent bridge: the governance problem in genomics. GDPR (EU)—Common Rule (U.S.). Diagram was refined and re-created with Claude Opus 5 (Anthropic) from an original designed by the authors.

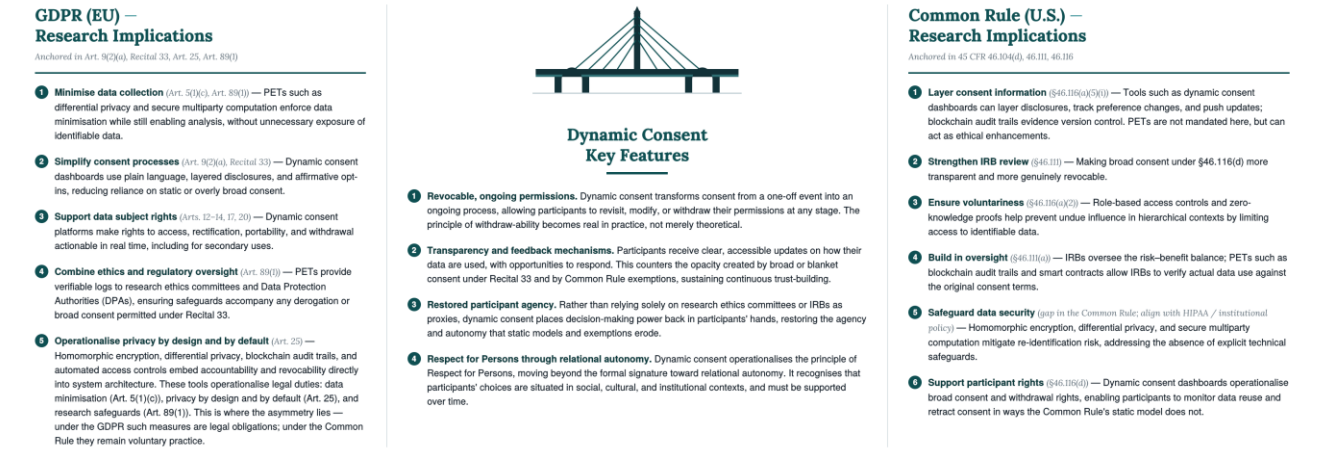

Figure 2. Dynamic governance bridge: repairing consent in genomics. Diagram was refined and re-created with Claude Opus 5 (Anthropic) from an original designed by the authors.

The article proceeds as follows. Section 2 develops the SCOT and PRP frameworks as analytical lenses. Section 3 sets out the doctrinal architecture of the GDPR and the U.S.C.R. and illustrates their divergence through the DeepMind and 23andMe cases. Section 4 moves from doctrinal divergence to governance response, interpreting the GDPR's cumulative legality obligations in genomic AI contexts through the lenses of SCOT and PRP. Section 5 develops the case for dynamic consent as a governance mechanism not an independent lawful basis in dual-regulation environments. Section 6 concludes.

2. Reconstructing consent and risk: SCOT and PRP as ethical and sociotechnical lenses

As illustrated by SCOT's classic bicycle case, governance categories such as 'consent' and 'risk' are institutionally co-constructed rather than fixed (See Box 1). PRP provides the normative benchmark (See Box 2), requiring relational autonomy and ongoing ethical engagement rather than one-off authorisation. Within this framework, consent is best understood not simply as a procedural requirement, but as a sociotechnical mechanism through which legitimacy, accountability, and trust are produced and maintained across evolving research contexts.

SCOT highlights how categories such as "broad consent" and "minimal risk" stabilise through institutional practice, while PRP emphasises that autonomy is relational, temporally extended, and shaped by conditions of participation. This combined perspective shifts the focus from consent as a discrete event to consent as an ongoing ethical relationship embedded within systems of governance. The socio-legal significance of this shift is not merely analytical. When consent functions as a governance mechanism rather than a one-off authorisation, it structures institutional responsibility, conditions the legitimacy of downstream data use, and provides a traceable basis for accountability over time. This is precisely what static consent frameworks fail to deliver as the DeepMind and 23andMe cases demonstrate in Section 3.3.

In genomic AI, this requires iterative consent that recognises autonomy as socially embedded and institution dependent. As Prinsen (2023) shows, dynamic consent[1] embodies this shift by linking privacy

[1] Dynamic consent is not itself a lawful basis under the GDPR and does not guarantee compliance. Rather, it functions as a governance mechanism that supports the implementation of existing legal obligations particularly transparency (Articles 12–14), accountability (Art 5(2)), data protection by design (Art 25), and the conditions for valid consent under Articles 6, 7, and 9.

and trust to participant control and ongoing engagement [10]. Weller *et al.*'s 'linked lives' analysis underscores that consent must account for family, social, and intergenerational ties, reinforcing PRP's demand for engagement that goes beyond static, front-loaded models [11]. Critically, dynamic consent is not an independent lawful basis under the GDPR. Its function is operational: it may support compliance with existing obligations, ongoing transparency under Articles 12–14, accountability under Article 5(2), purpose compatibility under Articles 6 (4) and 9 (2) (j) without substituting for them. Figure 3 synthesises these differences by contrasting how consent rules operate across the GDPR and the U.S.C.R., highlighting their distinct approaches to autonomy, safeguards, and downstream data use.

Two Regulatory Logics for Genomic and AI-Driven Health Research

Governance-by-design under the GDPR and the European Health Data Space, set against proceduralism and exemption under the U.S. Common Rule.

DIMENSION	GOVERNANCE-BY-DESIGN GDPR & EHDS (EU) Reg. (EU) 2016/679; Reg. (EU) 2025/327	PROCEDURALISM & EXEMPTIONS U.S. Common Rule 45 CFR 46, subpart A
Consent baseline	Consent is defined as freely given, specific, informed, and unambiguous (Art. 4(11)); explicit consent is required for genetic and health data (Art. 9(2)(a)).	Consent is front-loaded at enrolment under IRB oversight. No explicit-consent requirement attaches to de-identified or exempt studies.
Broad consent	Permitted only with safeguards — transparency, proportionality, pseudonymisation — operationalised through Arts. 13–14 and 89(1) (Recital 33).	Commonly accepted where data are coded or de-identified (§46.116(d)); participant re-engagement is limited.
Safeguards	Transparency duties are mandatory (Arts. 13–14); proportionality, minimisation, and pseudonymisation are required for research processing (Art. 89(1)). The EHDS adds a system-level ecosystem for secondary use: health data access bodies, an opt-out mechanism, and permit-based governance.	Relies on IRB discretion and general risk–benefit review (§46.111). The "minimal risk" standard is routinely applied even in genomic and AI contexts, where cumulative and downstream risk is poorly captured.
Autonomy and Respect for Persons	Autonomy and protection are embedded as enforceable duties, with dignity grounded in the Charter of Fundamental Rights (Recital 1). Governance-by-design creates institutional hooks for oversight that evolves with the research.	Autonomy is compressed into a discrete transaction at the point of consent; protection is delegated to IRB judgement. Relational and group-level risks are externalised rather than governed.
Regulatory logic	Precautionary, rights-based, and relational. Respect for Persons is embedded structurally, in both legal text and institutional architecture.	Efficiency-driven, procedural, and categorical. Respect for Persons is filtered through IRB practice rather than secured by structural guarantee.
Illustrative cases	**UK Biobank.** Explicit consent combined with Recital-33-compatible safeguards when cohort data are repurposed for AI development.‡	**All of Us.** Broad initial consent plus de-identification enabled secondary AI use without re-consent. **23andMe.** Commercial reuse permitted where datasets are deemed de-identified. Under the GDPR, renewed consent or demonstrable safeguards would be required.

‡ *UK Biobank operates under the UK GDPR and the Data Protection Act 2018 rather than the EU instrument; it is included for comparability of governance design, not of applicable law.*

The EHDS entered into force on 26 March 2025. Its secondary-use provisions apply from 26 March 2029, and those covering human genetic data from 26 March 2031 — the ecosystem described here is therefore prospective rather than currently operative.

Figure 3. Governance logics of the GDPR and U.S.C.R. in genomic AI. Diagram was refined and re-created with Claude Opus 5 (Anthropic) from an original designed by the authors.

3. Genomic doctrinal architecture of consent and secondary use in genomic AI under the GDPR and the U.S.C.R.

Genomic AI repurposes data, generates new inferences, and produces relational and intergenerational effects that static consent models struggle to anticipate [12]. These dynamics expose significant differences in how the GDPR and the U.S.C.R. conceptualise legality, consent, and secondary use. A clear doctrinal foundation is therefore required. The governance consequences of these differences are then assessed through the DeepMind and 23andMe cases in Section 3.3, before the normative reconstruction grounded in SCOT and PRP that follows.

3.1. The GDPR: principles, lawful bases, and conditions for processing genomic data

All processing under the GDPR is governed by the principles set out in Article 5, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, integrity and confidentiality, and accountability. Article 5(1)(b) establishes a conditional presumption of compatibility for further processing for scientific research purposes, provided that such reuse is supported by the safeguards required under Article 89(1), including data minimisation, pseudonymisation, and appropriate organisational

and ethical oversight. These safeguards are conditions of lawful research processing, not optional protections, and do not operate independently of the Regulation's general legality requirements.

Article 6 establishes the lawful bases for processing personal data. Where data are repurposed, Article 6(4) requires that secondary use be compatible with the original purpose, assessed through criteria including context, participant expectations, and safeguards. Where personal data were originally collected on the basis of consent under Article 6(1)(a), any further processing must remain within the scope of that consent; incompatible reuse requires fresh consent or an alternative lawful basis, including where data are repurposed for AI development or the generation of new inferences.

At a constitutional level, Article 8 of the EU Charter of Fundamental Rights functions as a primus inter pares among informational rights [13]. It requires that personal data processing be substantively justified through legality, proportionality, purpose limitation, and effective safeguards, rather than resting solely on procedural authorisation or individual consent. Genomic data constitute special-category data under Article 9 GDPR. Article 9(1) imposes a general prohibition on processing, lifted only where one of the conditions in Article 9(2) applies. Explicit consent under Article 9(2)(a) and the research condition under Article 9(2)(j) both operate within, and never displace, the safeguards mandated by Article 89(1) [14]. Article 9 therefore forms part of the GDPR's integrated legality architecture rather than functioning as a standalone or exceptional safeguard.

Articles 13 and 14 impose continuing transparency obligations that condition both the validity of consent and the lawfulness of secondary use. Controllers must disclose foreseeable further processing purposes, categories of recipients, and the existence of automated decision-making or profiling. These duties are anchored in Article 6(1)(a) and, for genomic data, Article 9(2)(a). Article 7 governs how consent operates in practice, requiring that it be freely given, specific, informed, and unambiguous; it places the burden of proof on controllers and requires that withdrawal be as easy as consent is given. Recitals 32, 42, and 43 clarify these requirements, particularly in contexts marked by institutional or informational power asymmetries.

Recital 33 performs a strictly interpretative function within this architecture: it does not authorise broader or open-ended processing, nor does it establish an independent legal basis for research involving genomic data It acknowledges that scientific purposes may evolve ex ante, while leaving the legality and limits of permissible processing to be determined entirely by the binding provisions of Articles 5, 6, 9, and 89(1) [15–17]. Broad consent remains compatible with the GDPR only where further processing is purpose-compatible, accompanied by continuing transparency under Articles 13 and 14, and subject to the proportional safeguards mandated by Article 89(1). Veit similarly shows that these cumulative safeguards embed consent within a dynamic governance model rather than treating it as a one-off authorization, confirming that Recital 33 operates as an interpretative constraint rather than a permissive gateway [18].

In legal terms, the GDPR operationalises core commitments associated with the principle of PRP by structuring consent, transparency, and legality as ongoing conditions of lawful processing rather than one-time procedural acts. Explicit consent requirements (Articles 6(1)(a), 7,9(2)(a)), continuing transparency obligations (Articles 13 and 14), and the heightened legality and safeguard requirements governing special-category data processing (Articles 9(2)(j), 89(1)) collectively function to preserve data-subject agency, enable meaningful re-evaluation of participation over time, and constrain institutional power in contexts marked by informational asymmetry and cumulative risk [19]. Together,

these provisions require proportionality, ongoing transparency, and context-sensitive oversight in research settings.

Recent EU legislation reinforces rather than alters this doctrinal structure. The European Health Data Space Regulation (EHDS) 2025 established a harmonized mechanism for secondary-use permits, data-access bodies, interoperability standards, and enhanced user controls, operating alongside the GDPR's legality framework rather than replacing it [20,21]. Similarly, the EU AI Act (Reg. 2024/1689) introduces additional oversight obligations for high-risk AI systems, including documentation, risk assessment, post-market monitoring, thereby strengthening governance conditions for genomic AI without modifying the core requirements of Articles 5, 6, 7, 9, 13 and 14, or 89(1) GDPR [22,23]. Crucially, both instruments extend rather than dilute the GDPR's commitment to layered, ongoing safeguards reinforcing the cumulative governance architecture that constrains secondary use of genomic data in AI systems [24].

Failures to satisfy these cumulative requirements carry concrete consequences, as illustrated by the DeepMind–Royal Free NHS case, where the absence of transparency, purpose compatibility, and appropriate safeguards led the UK Information Commissioner's Office to find the processing unlawful [25]. The critical point is not merely doctrinal but functional: this architecture requires that consent rules operate as ongoing governance conditions rather than one-off authorisations. Broad consent remains compatible with the GDPR only where further processing is purpose-compatible, accompanied by continuing transparency, and subject to the proportional safeguards mandated by Article 89(1); it cannot displace the principles in Article 5 [26]. The doctrinal framework established in this section is the definitive account of the GDPR's cumulative legality architecture and is cross-referenced rather than restated in subsequent sections. The full analysis of this case, and its implications for how the GDPR's cumulative architecture functions as a governance mechanism, is set out in Section 3.3.

3.2. The U.S.C.R.: static consent, identifiability, and categorical exemptions

By contrast, the U.S.C.R. reflects a predominantly procedural account of the PRP. While it requires initial informed consent, its exemption framework under Section 46.104(d) frequently removes research involving de-identified biospecimens from continuing oversight [27,28]. This exemption-based structure means that genomic data stored in biobanks may be reused for AI research without re-contacting participants. This applies even where new inferences about disease risk or familial traits accumulate over time. The result is a structural gap with direct consequences for how responsibility is allocated and whether participants retain any meaningful oversight of subsequent data uses.

Genomic findings such as those associated with Lynch syndrome implicate families and identifiable subpopulations, generating cumulative and intergenerational risks that reflect the inherently relational and population-based nature of predictive genomics [29]. The U.S.C.R. does not adequately account for these risks. Its structure is anchored in a front-loaded model of autonomy built around one-off consent and categorical exemptions [30]. Section 46.104(d) plays a decisive role it permits secondary research using identifiable private information or biospecimens without consent where specified recording or HIPAA conditions are met. Sections 46.104(d)(7) and (8) introduce a broad-consent pathway for storage and secondary use, but uptake remains limited in practice [31–33]. As a result, much AI-driven reuse proceeds outside sustained ethical oversight [34]. This marks a structural divergence from the GDPR

which, as established in Section 3.1, embeds the PRP within layered and evolving obligations rather than relying on static consent and exemptions [35].

The U.S.C.R.'s definitional categories further amplify these limitations. Under Section 46.102(e), biospecimens are considered identifiable only where identity can be 'readily ascertained,' a threshold increasingly unstable in genomic AI, where re-identification is often technically feasible. The 'minimal risk standard in Section 46.102(j) remains confined to individual harms and does not capture familial, group, or intergenerational risks intrinsic to genomic data [36]. Scholars have shown that, taken together, these provisions create a consent exemption architecture in which substantial AI-driven secondary use falls outside IRB review altogether [31,32,37].

Consent itself is treated under Section 46.116 as a discrete procedural event, supported by initial IRB review but without requirements for ongoing engagement as data are reused or new inferences emerge [31–33,38,39]. The U.S.C.R. contains no compatibility test for downstream reuse and no analogue to the GDPR's provisions governing purpose compatibility, continuing transparency, or proportional safeguards. NIH policy reinforces these structural limits. The Genomic Data Sharing (GDS) Policy promotes broad expectations of future data use but does not require renewed or ongoing participant engagement [39]. Controlled-access repositories such as dbGaP regulate initial access but do not constrain downstream inference or analytics once data are released. As Byrd *et al.* note, such mechanisms mitigate front-end re-identification risks but cannot restrict the analytical capacities of secondary users or the generation of new inferences [40,41]. Although NIH guidance acknowledges relational risks, the U.S.C.R. remains centered on individual consent and de-identification, offering no mechanisms to address cumulative, familial, or intergenerational harms. In this sense, the structure of Section 46.104(d) is decisive [37,42].

The 23andMe controversies illustrate how this structure operates in a commercial context. One-off consent authorised extensive inference generation, data licensing, and cross-sector analytics without renewed engagement, compatibility assessment, or sustained oversight. These outcomes were not incidental but structural produced collectively by the U.S.C.R.'s exemption framework, identifiability threshold, and absence of a compatibility test [31,33,37,38]. The full analysis of this case is set out in Section 3.3.

3.3. Case studies: how doctrinal divergence shapes real-world governance outcomes

The cases examined here demonstrate how the doctrinal divergences established in Sections 3.1 and 3.2 translate into concrete governance outcomes showing what follows, in practice, when consent rules operate as cumulative governance constraints under the GDPR, and as front-loaded authorisations under the U.S.C.R.

(A) DeepMind–royal free NHS: GDPR compatibility and transparency in practice

The Royal Free London NHS Foundation Trust transferred approximately 1.6 million patient records to Google DeepMind to develop and test the Streams clinical decision-support tool. Patients were not informed, and processing expanded beyond direct care to algorithm development. In this context, consent rules were functioning or failing to function as governance mechanisms: they were the legal instruments through which the boundaries of permissible data use should have been defined, participant expectations structured, and institutional responsibility allocated. Under the GDPR, this

constituted ‘further processing’ within Article 5(1)(b), triggering Article 6(4)’s compatibility assessment because the AI-related use diverged materially from the original clinical purpose [25].

As the data comprised special-category health information, reliance on Article 9(2)(j) required demonstrable safeguards under Article 89(1), including minimisation and proportional oversight. The absence of patient notification breached the transparency duties in Articles 13 and 14. The UK Information Commissioner’s Office found the processing unlawful, incompatible with purpose limitation, and lacking a valid lawful basis. This case illustrates what follows when the GDPR’s cumulative requirements are not satisfied: the transition from clinical care to AI development was not properly justified under the compatibility test, patients were not informed, and appropriate safeguards were not demonstrably in place. As a result, consent rules failed to perform their governance function they neither structured participant expectations about secondary use nor allocated institutional responsibility for the transition from clinical care to AI development. This also underscores the risk, identified by Shahizam, that GDPR formalism can emerge when broad consent is treated as a substitute for meaningful participant agency, a risk that is institutional rather than merely individual [13].

(B) 23andMe: exemptions, broad consent, and structural gaps under the U.S.C.R.

By contrast, 23andMe collected genomic data from millions of individuals through direct-to-consumer testing, using one-off commercial consent to authorise internal research, data licensing, and commercial partnerships. Here, consent rules operated as front-loaded authorisations instruments that permitted expansive downstream use at the point of collection without structuring ongoing participant expectations, allocating responsibility for subsequent data use, or providing any mechanism for reassessment as risks accumulated. As most of the activities occurred outside federally funded research, downstream uses generally fell outside U.S.C.R. oversight and IRB review [43,44]. Subsequent controversies including credential-stuffing breaches, covert secondary uses, and law-enforcement access requests demonstrate how, once data leave the initial collection context, extensive inference generation and cross-sector analytics proceed without renewed consent, compatibility assessment, or sustained oversight [36,45–47].

These outcomes reflect the combined effect of three structural features of the U.S.C.R.: Sections 46.104(d)(4)’s broad exemptions, Section 46.102(e)’s narrow identifiability threshold, and the absence of any analogue to Article 6(4)’s compatibility test. Together, these features allow one-off consent to authorise expansive downstream uses despite persistent relational and intergenerational risks [48,49]. In this case, consent rules operate as front-loaded authorisations: once consent is obtained at the point of collection, downstream uses proceed without requirements for renewed engagement, compatibility assessment, or reassessment of risk. Responsibility for downstream use remains diffuse, leaving participants without visibility or control over subsequent data uses.

Taken together, these cases expose a fundamental mismatch between genomic AI’s dynamic risk profile and the static legal categories governing consent under both regimes. As wider scholarship confirms, genomic data implicate ‘linked lives’ across families and generations rendering one-off authorisation ethically insufficient and responsibility for downstream use structurally diffuse [10,11]. Andreotta *et al.* further show how AI and Big Data infrastructures erode the informational assumptions underpinning traditional informed consent meaning that even where consent was genuinely informed at the point of collection, it cannot remain so as data are repurposed and new inferences generated [50]. These governance fractures are depicted in Figure 1 and summarised in Figure 3. The GDPR’s model

embeds compatibility, transparency, and ongoing safeguards more clearly than frameworks relying on front-loaded authorisation and categorical exemption. It more effectively allocates responsibility and sustains accountability over time.

4. Consent governance in genomic AI: SCOT, PRP, and the GDPR's cumulative obligations

The doctrinal and empirical analysis in Section 3 reveals parallel but distinct limitations in both frameworks when read through SCOT and PRP. From a PRP perspective, genomic decision-making is relational and temporally extended: preferences evolve while familial and intergenerational implications accumulate over time [51]. SCOT complements this by showing how categories such as 'minimal risk,' 'exempt,' and 'broad consent' stabilise through administrative routine, often failing to reflect the lived risks of genomic AI.

The GDPR provides a stronger structural foundation for relational governance. Yet as the DeepMind case illustrated in Section 3.3, it remains vulnerable to procedural formalism when broad consent substitutes for meaningful participant agency and safeguards are reduced to formal checklists [13,25]. The U.S.C.R. entrenches a procedural, individual-centred model of autonomy in which 'exempt' and 'minimal risk' have hardened into administratively convenient categories despite their poor fit with genomic inference practices. The 23andMe case illustrated this concretely: mechanisms for renewed engagement, compatibility assessment, and risk reassessment were structurally absent [36,43]. Neither framework fully accounts for the temporally extended and relational nature of genomic AI underscoring the need for governance mechanisms capable of sustained engagement, transparency, and accountability. Genomic AI generates risks that are dynamic, cumulative, and relational, extending beyond individuals to families and communities. From the perspective of the PRP, consent cannot be reduced to a single legal act; it must operate as an ongoing ethical relationship that remains responsive to evolving uses, vulnerabilities, and downstream consequences. These features place pressure on static consent models and require careful interpretation of the GDPR's research framework the doctrinal basis of which was established in Section 3.1 and the governance consequences of which were demonstrated through the case studies in Section 3.3.

4.1. Transparency, consent validity, and secondary use

Articles 13 and 14 impose continuing transparency obligations that condition both the validity of consent and the lawfulness of secondary use. Controllers must disclose foreseeable further processing purposes, categories of recipients, and the existence of automated processing or profiling. These duties are structurally linked to Article 6(1)(a) and, for genomic data, Article 9(2)(a) and their breach, as the DeepMind case demonstrated, renders processing unlawful regardless of institutional partnership arrangements. Article 7 governs how consent operates in practice. It requires that consent be freely given, specific, informed, and unambiguous, places the burden of proof on the controller, and mandates that withdrawal be as easy as giving consent. Recitals 32, 42, and 43 of the GDPR clarify these requirements. Recital 32 addresses the granularity and specificity of consent, requiring that it cover all processing activities carried out for the same purpose. Recital 42 addresses the conditions for demonstrating valid consent, placing the burden of proof on the controller. Recital 43 addresses the problem of power asymmetry between data subjects and institutional controllers, providing that consent cannot serve as a

valid legal ground where such imbalance exists. All three are directly relevant in genomic AI research contexts, where institutional power, informational asymmetry, and the breadth of potential data use create precisely the conditions these recitals were designed to address.

4.2. Compatibility and evolving AI use

Where genomic data are repurposed for AI model development or inference generation, Article 6(4)'s compatibility assessment becomes central. The assessment requires consideration of the relationship between purposes, the context of data collection, the nature and sensitivity of the data, the foreseeable consequences for data subjects, and the presence of safeguards [52]. These factors take on heightened importance in genomic AI because inferential, familial, and intergenerational risks render secondary uses ethically and contextually distinct as the 23andMe case illustrated through the absence of any equivalent compatibility mechanism under the U.S.C.R.

Recent European Data Protection Board guidance on privacy risks in large language models confirms that AI systems generate evolving and cumulative risks requiring ongoing assessment, documentation, and mitigation across the system lifecycle [53]. This guidance is interpretative in nature and does not modify the binding legal framework of the GDPR, but clarifies how existing obligations, purpose limitation, lawfulness, and proportionality apply in AI contexts. It therefore underscores the operational necessity of governance mechanisms capable of sustaining transparency, accountability, and proportional safeguards over time.

These concerns are especially acute in genomic contexts. Data collected from one individual can generate inferences about their family members, be reused across multiple studies over time, and produce harms that extend far beyond the original consent context without triggering any additional legal obligations under the GDPR. Shabani and Marelli (2019) provide a foundational explanation for why static consent models are structurally inadequate in this context: de-identification of genomic data cannot be achieved once and for all but must be periodically reassessed at every stage of processing, in line with the GDPR's risk-based accountability obligations under Articles 5(2) and 24. This means that consent given at the point of collection cannot remain adequate as data are reprocessed, linked to other datasets, and generate new inferences over time [54].

Empirical evidence from the HealthData@EU Cancer Genomics Use Case confirms these governance challenges in practice. Royo *et al.* (2025) found that across Belgium, Denmark, Norway, and BBMRI-ERIC, existing consent rarely covered secondary genomic use adequately. In Norway required re-consent from living patients and relatives of deceased patients, Denmark required renewed consent for exploratory studies, and Belgium faced commercial restrictions on data access [55]. After more than two years, data remained unavailable in most participating institutions, illustrating that even within GDPR-governed jurisdictions, purpose compatibility and ongoing transparency obligations are difficult to operationalise without structured governance mechanisms capable of sustaining participant engagement across evolving research contexts [55].

4.3. SCOT, PRP, and the risk of formalism

SCOT helps explain how categories such as 'broad consent,' 'compatible purpose,' and 'research use' may stabilise through institutional routine in ways that drift from their protective intent. Without

sustained engagement mechanisms, those routines tend to consolidate consent and safeguard requirements into symbolic compliance artefacts formally present but substantively hollow. PRP exposes the ethical consequences of such drift, requiring interpretations that preserve relational autonomy through ongoing engagement rather than one-off authorisation. These risks are not merely theoretical they were illustrated concretely by the DeepMind and 23andMe cases in Section 3.3, and they become acute in genomic AI where downstream inferences and intergenerational effects accumulate over time.

Dynamic consent may provide a governance mechanism capable of aligning the GDPR's cumulative legal architecture with the relational obligations demanded by the PRP but, as established in Section 2, it does not constitute an independent lawful basis and does not substitute for the requirements of Articles 5, 6, 7, 9, or 89(1). Its function is operational and supportive, sustaining the conditions that the GDPR's legality architecture requires without replacing them. In research contexts, it may support the proportional safeguards required by Article 89(1) and help ensure that processing remains within the limits of Article 9(2)(j). By enabling renewed transparency, participant re-engagement, and traceable decision points, it may also reduce the risk that Recital 33 is interpreted expansively as established in Section 3.1, this interpretative risk is real and institutionally consequential. Dynamic consent therefore may support, rather than replace, the GDPR's legality architecture by sustaining accountability and participant involvement as scientific uses evolve.

Governance failures illustrate the consequences of static consent, as established through the DeepMind and 23andMe cases in Section 3.3 rather than restated here. Evidence from the All of Us programme similarly indicates that one-off consent cannot prepare participants for AI-driven secondary uses or cumulative relational risks. Empirical studies confirm that dynamic consent models could enhance comprehension, trust, and participant agency [15,17,56]. Figure 2 illustrates how these doctrinal requirements can be operationalised in practice without displacing the GDPR's legality architecture.

5. Dynamic consent as an ethically responsive alternative in dual regulation environments

Building on the doctrinal and normative analysis in Sections 3 and 4, this section develops the case for dynamic consent as a governance mechanism in dual-regulation environments such as Qatar. Dynamic consent should be understood not as a substitute for the GDPR's operative provisions but as a governance mechanism that may support compliance with Articles 5, 6, 9, 12–14, and 89(1). As established in Section 2, its value lies in operationalising existing obligations in contexts where purposes evolve, risks accumulate, and participant expectations cannot be fully specified ex ante. This function is particularly salient in genomic AI contexts marked by structural or institutional power imbalance precisely the conditions under which the Court of Justice of the EU and the EDPB have emphasised that consent must be assessed substantively, with attention to asymmetries that undermine whether it is genuinely 'freely given' [57].

Under the GDPR, consent must be specific, informed, freely given, and unambiguous, while Articles 12–14 impose continuing transparency obligations rather than a one-off disclosure event. Dynamic consent could operationalise these requirements by enabling iterative information flows, renewed engagement, granular permissions, and real-time withdrawal, thereby reinforcing accountability under Article 5(2) and controller duties under Articles 24 and 25. Genomic AI heightens the need for adaptive governance, as genomic data are inherently identifying, relational, and inference-generating, often

extending beyond initial research purposes [58–62]. Although Article 6(4)'s compatibility test and Article 9(2)(j)'s reliance on Article 89(1) safeguards partially anticipate these dynamics, neither requires ongoing participant engagement a gap that dynamic consent may be well positioned to address.

The clinical and commercial governance failures established in Section 3.3 illustrate why these matters in practice. In clinical settings, the DeepMind–Royal Free case illustrates how the absence of a dynamic consent mechanism meant that the transition from direct care to AI development proceeded without renewed participant engagement, transparency, or compatibility assessment [25]. A structured iterative consent infrastructure could have mitigated these failures by conditioning further processing on explicit participant notification and re-engagement for instance, by requiring patients to be informed when their records moved from direct clinical use to algorithm development, and providing a mechanism through which they could review, query, or withdraw their participation at that transition point.

SCOT clarifies why these failures persist: categories such as 'consent,' 'minimal risk,' and 'compatible purpose' tend to stabilize through institutional routine, becoming administrative artefacts detached from their protective rationale. As established in Section 2 and 4, PRP sharpens the normative critique by emphasising relational autonomy and recognising that preferences evolve and familial implications unfold over time [1,63–65]. Dynamic consent directly addresses these concerns by treating consent as an ongoing institutional relationship, with empirical evidence demonstrating improved comprehension, trust, and participant engagement [58,62].

The case for dynamic consent is especially acute in dual-regulation environments such as Qatar, where GDPR-style safeguards coexist with U.S.C.R. exemptions a structural problem identified in the Introduction and developed through the comparative analysis in Sections 3 through 5. As McKay *et al.* (2023) and Walch-Patterson (2020) show, exemptions under Section 104(d) frequently remove AI-driven studies from continuing oversight, allowing relational and intergenerational risks to accumulate without institutional scrutiny [31,66]. Dynamic consent may contribute to addressing these gaps by reinstating structured transparency, participant re-engagement, and auditability even where formal legal obligations under the U.S.C.R. are limited. The persistence of governance gaps even within GDPR-governed jurisdictions underscores this point. Royo *et al.* (2025) demonstrate that Article 51(4) of the European Health Data Space (EHDS) permits Member States to impose additional safeguards for genomic data, meaning that national heterogeneity in consent requirements persists even after EHDS implementation. In dual-regulation environments such as Qatar, where GDPR-style obligations coexist with U.S.C.R. exemptions and no equivalent EHDS harmonisation mechanism applies, these governance gaps are structurally compounded. Dynamic consent may provide a cross-jurisdictional governance floor capable of sustaining transparency, participant re-engagement, and auditability regardless of which formal legal framework governs any particular data flow [55].

Empirical implementations, such as the CTRL platform within Australian Genomics demonstrates that consent management, access controls and participant involvement can be operationalised at scale [67]. Piasecki and Chen further argue that GDPR data-protection-by-design obligations under Article 25 require embedding protective defaults within technical infrastructures a function that dynamic consent is well positioned to support by enabling these safeguards to be operationalised within technological systems [68].

In summary, dynamic consent may offer a principled governance response for genomic AI capable of operationalising relational autonomy, addressing the limitations of static consent models, and

supporting accountability in the face of cumulative and intergenerational risk. Its value lies not in replacing existing legal frameworks but in sustaining the conditions they require in practice.

6. Conclusion

This article has shown that the central challenge in genomic AI governance lies not in the absence of consent but in how consent rules are structured and operationalised across regulatory frameworks. This structural problem has concrete governance consequences, as illustrated by the DeepMind and 23andMe cases discussed in Section 3.3.

Under the GDPR, consent is embedded within a cumulative legality architecture, established doctrinally in Section 3.1, that requires compatibility, transparency, and safeguards. Under the U.S.C.R., by contrast, consent operates primarily as a front-loaded authorisation, permitting downstream use without sustained oversight. These differences reflect deeper divergences in regulatory logic between a GDPR model grounded in compatibility, transparency, and ongoing safeguards and a U.S. model structured around exemptions and de-identification, rather than mere variations in legal technique [16,69].

As established through the SCOT analysis in Section 2, categories such as broad consent, minimal risk, and compatible purpose can become stabilised through institutional practice and drift from their protective intent [69–71]. The PRP analysis developed in Sections 2 and 4 sharpens this critique by emphasising that autonomy is relational and temporally extended, requiring governance structures capable of responding to evolving risks, inferences, and social implications [63,64,72].

These dynamics were illustrated concretely in Section 3.3. The DeepMind–Royal Free case showed how the GDPR's cumulative architecture exposed governance failures relating to transparency and purpose limitation. The 23andMe controversies showed how the U.S.C.R.'s exemption-based structure allowed front-loaded authorisation to substitute for ongoing accountability. In dual-regulation environments such as Qatar, both sets of dynamics can occur simultaneously, making the absence of a cross-jurisdictional governance mechanism a structural rather than merely incidental problem, as demonstrated by the comparative analysis in Sections 3–5.

As established in Section 2, dynamic consent does not constitute an independent lawful basis under the GDPR and does not substitute for the requirements of Articles 5, 6, 7, 9, or 89(1). It is a governance mechanism whose value lies in operationalising those requirements in practice by enabling ongoing transparency, participant engagement, and traceable decision-making in contexts where data use evolves over time [65,73]. While privacy-enhancing technologies play an important role in mitigating risks such as re-identification and data breaches, they cannot replace governance mechanisms; the effective protection of genomic data requires integrating these technologies within frameworks capable of addressing the relational, contextual, and long-term implications of data use [74,75].

Regulatory fragmentation compounds these challenges. Divergent consent standards, identifiability thresholds, and cross-border rules allow genomic data to circulate without coherent oversight. As Figure 3 demonstrates, this fragmentation corresponds to a deeper divergence between a GDPR model grounded in compatibility and safeguards and a U.S. model structured around exemptions and de-identification—a divergence that Figures 1 and 2 jointly illustrate at the level of governance design.

The contribution of this article is therefore to reconceptualise consent rules as governance mechanisms. Consent must do more than authorise data use at a single point in time; it must structure responsibility, mediate expectations, and sustain meaningful participant involvement as data are reused

and reinterpreted. Without this shift, the governance gaps identified through the comparative analysis, the case studies, and the SCOT and PRP frameworks will persist. Dynamic consent should therefore be understood not as a substitute for existing legal frameworks, but as a potential governance mechanism that may support the GDPR's requirements for transparency, accountability, and ongoing participant engagement in contexts where data use evolves over time.

Declaration of generative AI and AI-assisted technologies

During the preparation of this manuscript, the authors used Claude Opus 5 (Anthropic) only for drafting and language polishing purposes, and to refine the diagrams for clarity. All intellectual content was developed by the authors. The authors take full responsibility for the content of the manuscript.

Acknowledgments

This research did not receive any specific funding. We acknowledge the research compliance team at WCM-Q in their continued efforts to build robust human research participant protections at WCM-Q and within Qatar.

Authors' contribution

Nabila Khwaja: methodology, formal analysis, investigation, writing, review—editing; Amal Robay: project administration, supervision, resources. All authors have read and agreed to the published version of the manuscript.

Conflicts of interest

The authors declare that there are no conflicts of interest related to this research. The study was conducted independently, and no funding, employment, consulting fees, research contracts, stock ownership, patent licenses, honoraria, or advisory affiliations influenced the design, analysis, or interpretation of the study.

References

[1] Delgado J. Re-thinking relational autonomy: challenging the triumph of autonomy through vulnerability. *Bioeth. Update* 2019, 5(1):50–65.
[2] Herring J. *Law and the Relational Self*. Cambridge: Cambridge University Press, 2019.
[3] Mühlhoff R, Ruschemeier H. Updating purpose limitation for AI: a normative approach from law and philosophy. *Int. J. Law Inf. Technol.* 2025, 33:eaaf003.
[4] Lowrance WW, Collins FS. Identifiability in genomic research. *Science* 2007, 317(5838):600–602.
[5] Moulaei K, Akhlaghpour S, Fatehi F. Patient consent for the secondary use of health data in artificial intelligence (AI) models: a scoping review. *Int. J. Med. Inform.* 2025, 198:105872.
[6] Struelens MJ, Ludden C, Werner G, Sintchenkoet V, Jokelainen P, *et al.* Real-time genomic surveillance for enhanced control of infectious diseases and antimicrobial resistance. *Front. Sci.* 2024, 2:1298248.

[7] May T, Zusevics KL, Derse A, Strong KA, Jeruzal J, *et al.* The limits of traditional approaches to informed consent for genomic medicine. *HEC Forum* 2014, 26(3):185–202.
[8] Passi S, Barocas S. Problem formulation and fairness. In *Proceedings of the conference on fairness, accountability, and transparency*, New York, USA, January 29–31, 2019.
[9] LeCompte LL, Young SJ. Revised common rule changes to the consent process and consent form. *Ochsner J.* 2020, 20(1):62–75.
[10] Prinsen L. Reconsidering consent for biomedical research using human biological material and associated data. *S. Afr. J. Sci.* 2023, 119(11–12):1–4.
[11] Weller S, Lyle K, Lucassen A. Re-imagining 'the patient': linked lives and lessons from genomic medicine. *Soc. Sci. Med.* 2022, 297:114806.
[12] Smit AK, Gokoolparsadh A, McWhirter R, Newett L, Milch V, *et al.* Ethical, legal and social issues related to genetics and genomics in cancer: a scoping review and narrative synthesis. *Genet. Med.* 2024, 26(12):101270.
[13] Shahizam S. Putting consent in its place: proceduralism and paternalism in data protection law. *LSE Law Rev.* 2021, 6(3):246–265.
[14] Staunton C, Slokenberga S, Parziale A, Mascalzoni D. Appropriate safeguards and article 89 of the GDPR: considerations for biobank, databank and genetic research. *Front. Genet.* 2022, 13:719317.
[15] Budin-Ljøsne I, Teare HJ, Kaye J, Beck S, Bentzen HB, *et al.* Dynamic consent: a potential solution to some of the challenges of modern biomedical research. *BMC Med. Ethics* 2017, 18(1):1–10.
[16] Hallinan D. Broad consent under the GDPR: an optimistic perspective on a bright future. *Life Sci. Soc. Policy* 2020, 16(1):1.
[17] Teare HJ, Prictor M, Kaye J. Reflections on dynamic consent in biomedical research: the story so far. *Eur. J. Hum. Genet.* 2021, 29(4):649–656.
[18] Veit RD. Safeguarding regional data protection rights on the global internet—the European approach under the GDPR. In *Personality and Data Protection Rights on the Internet: Brazilian and German Approaches*. Cham: Springer, 2022.
[19] Tamburri DA. Design principles for the General Data Protection Regulation (GDPR): a formal concept analysis and its evaluation. *Inf. Syst*. 2020, 91:101469.
[20] Commission E. European Health Data Space Regulation (EHDS). 2025. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en (accessed on 11 March 2025).
[21] Slokenberga S, Cathaoir KÓ, Shabani M. *The European Health Data Space: Examining a New Era in Data Protection*. London:Taylor & Francis, 2025.
[22] Smuha NA. Regulation 2024/1689 of the Eur. Parl. & Council of June 13, 2024 (EU artificial intelligence act). *Int. Leg. Mater.* 2025, 64(5):1234–1381.
[23] Kop M. EU artificial intelligence act: the european approach to AI. 2021. Available: https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai/ (accessed on 18 April 2025).
[24] Petročnik T, Palmieri S, Marot JA. The AI act and european health data space proposal: seeing 'AI to AI'with each other? 2023. Available: https://www.europeanlawblog.eu/pub/the-ai-act-and-european-health-data-space-proposal-seeing-ai-to-ai-with-each-other/release/1 (accessed on 16 May 2025).

[25] Powles J, Hodson H. Google deepmind and healthcare in an age of algorithms. *Health Technol.* 2017, 7(4):351–367.
[26] Mondschein CF, Monda C. The EU's General Data Protection Regulation (GDPR) in a research context. In *Fundamentals Of Clinical Data Science*. Cham: Springer Nature, 2019.
[27] Doksum T, Jarboe C. Exempt research. In *Institutional Review Board: Management and Function*. Burlington: Jones & Bartlett Learning, 2021.
[28] Lorenzo D, Esquerda M, Bofarull M, Cusi V, Roig H, *et al.* The reuse of genetic information in research and informed consent. *Eur. J. Hum. Genet.* 2023, 31(12):1393–1397.
[29] Hall WD, Morley KI, Lucke JC. The prediction of disease risk in genomic medicine: scientific prospects and implications for public policy and ethics. *EMBO Rep.* 2004, 5(S1):S22–S26.
[30] Lynch HF, Wolf LE, Barnes M. Implementing regulatory broad consent under the revised common rule: clarifying key points and the need for evidence. *J. Law Med. Ethics* 2019, 47(2):213–231
[31] Walch-Patterson A. Exemptions and limited institutional review board review: a practical look at the 2018 common rule requirements for exempt research. *Ochsner J.* 2020, 20(1):87–94.
[32] Meyer MN. There oughta be a law: when does (n't) the US Common Rule apply? *J. Law Med. Ethics* 2020, 48(S1):60–73.
[33] Sobel ME, Dreyfus JC. Disruptive influences on research in academic pathology departments: Proposed changes to the common rule governing informed consent for research use of biospecimens and to rules governing return of research results. *Am. J. Pathol.* 2017, 187(1):4–8.
[34] Davtyan T. The US approach to AI regulation: federal laws, policies, and strategies explained. *J. Law Technol. Internet* 2025, 16(2):223.
[35] Levine DS, Drossman DA. Addressing misalignments to improve the US health care system by integrating patient-centred care, patient-centred real-world data, and knowledge-sharing: a review and approaches to system alignment. *Discover Health Syst.* 2022, 1(1):8.
[36] Chapman CR, Quinn GP, Natri HM, Berrios C, Dwyer P, *et al.* Consideration and disclosure of group risks in genomics and other data-centric research: does the common rule need revision? *Am. J. Bioeth.* 2025, 25(2):47–60.
[37] Evans BJ. Power to the people: data citizens in the age of precision medicine. *Vand. J. Ent. Technol. Law* 2017, 19(2):243.
[38] McGuire AL, Roberts J, Aas S, Evans BJ. Who owns the data in a medical information commons? *J. Law Med. Ethics* 2019, 47(1):62–69.
[39] Dyke SO. Genomic data access policy models. In *Responsible Genomic Data Sharing*. London: Elsevier, 2020.
[40] Quinn P, Quinn L. Big genetic data and its big data protection challenges. *Comput. Law Secur. Rev.* 2018, 34(5):1000–1018.
[41] Byrd JB, Greene AC, Prasad DV, Jiang X, Greene CS. Responsible, practical genomic data sharing that accelerates research. *Nat. Rev. Genet*. 2020, 21(10):615–629.
[42] Froomkin AM. Big data: destroyer of informed consent. *Yale J. Law Technol.* 2019, 21:27.
[43] Allyse M. 23 and me, we, and you: direct-to-consumer genetics, intellectual property, and informed consent. *Trends Biotechnol.* 2013, 31(2):68–69.
[44] Doerr M, Meeder S. Big health data research and group harm: the scope of IRB review. *Ethics Hum. Res.* 2022, 44(4):34–38.

[45] Kirby E, Tassé AM, Zawati M, Knoppers BM. Data access and sharing by researchers in genomics. 2018. Available: https://genomequebec.com/wp-content/uploads/2023/04/35_en-1.pdf (accessed on 22 April 2023).
[46] Dove ES, Joly Y, Tassé AM, Knoppers BM. Genomic cloud computing: legal and ethical points to consider. *Eur. J. Hum. Genet.* 2015, 23(10):1271–1278.
[47] Kwon D. What went wrong at 23andMe? Why the genetic-data giant risks collapse. Nature 2025, 638(8049):14–15.
[48]Doerr M, Moore S, Barone V, Sutherland S, Bot BM, *et al.* Assessment of the all of us research program's informed consent process. *AJOB Empir. Bioeth.* 2021, 12(2):72–83.
[49] Hayden EC. The rise and fall and rise again of 23andMe. *Nature* 2017, 550(7675):174–177.
[50] Andreotta AJ, Kirkham N, Rizzi M. AI, big data, and the future of consent. *AI Soc.* 2022, 37(4):1715–1728.
[51] Horton R, Lucassen A. Consent and autonomy in the genomics era. *Curr. Genet. Med. Rep.* 2019, 7(2):85–91.
[52] Shabani M, Dove ES, Murtagh M, Knoppers BM, Borry P. Oversight of genomic data sharing: what roles for ethics and data access committees? *Biopreserv. Biobank.* 2017, 15(5):469–474.
[53] Barberá I. AI privacy risk & mitigations-Large Language Models (LLMs). 2025. Available: https://www.edpb.europa.eu/system/files/documents/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf (accessed on 25 November 2025).
[54] Shabani M, Marelli L. Re-identifiability of genomic data and the GDPR: assessing the re-identifiability of genomic data in light of the EU General Data Protection Regulation. *EMBO Rep.* 2019, 20(6):EMBR201948316.
[55] Royo R, Garcia E, Schlünder I, Hilmarsen C, Thomsen MK, *et al.* Genomic data sharing in research across Europe: legal challenges and upcoming opportunities within the European Health Data Space. *Eur. J. Public Health* 2025, 35(Supplement_3):iii25–iii31.
[56] Kaye J, Whitley EA, Lund D, Morrison M, Teare H, *et al.* Dynamic consent: a patient interface for twenty-first century research networks. *Eur. J. Hum. Genet.* 2015, 23(2):141–146.
[57] Groos D, Veen EV. Anonymised data and the rule of law. *Eur. Data Prot. L. Rev.* 2020, 6:498–508.
[58] Kaye J. The tension between data sharing and the protection of privacy in genomics research. *Annu. Rev. Genom. Hum. Genet.* 2012, 13(1):415–431.
[59] Anderlik MR, Rothstein MA. Privacy and confidentiality of genetic information: what rules for the new science? *Annu. Rev. Genom. Hum. Genet.* 2001, 2(1):401–433.
[60] Resnik DB. Privacy and confidentiality. In *The Ethics of Research with Human Subjects: Protecting People, Advancing Science, Promoting Trust*. Cham: Springer Nature, 2025.
[61] Bonomi L, Huang Y, Ohno-Machado L. Privacy challenges and research opportunities for genomic data sharing. *Nat. Genet.* 2020, 52(7):646–654.
[62] Knoppers BM, Beauvais MJ. Three decades of genetic privacy: a metaphoric journey. *Hum. Mol. Genet.* 2021, 30(R2):R156–R160.
[63] Mackenzie C, Stoljar N. Introduction: autonomy refigured. In Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self. New York: Oxford University Press, 2000.
[64] Stoljar N. Informed consent and relational conceptions of autonomy. *J. Med. Philos.* 2011, 36(4):375–384.

[65] Dankar FK, Gergely M, Malin B, Badji R, Dankar SK, *et al.* Dynamic-informed consent: a potential solution for ethical dilemmas in population sequencing initiatives. *Comput. Struct. Biotechnol. J.* 2020, 18:913–921.

[66] McKay F, Williams BJ, Prestwich G, Bansal D, Treanor D, *et al.* Artificial intelligence and medical research databases: ethical review by data access committees. *BMC Med. Ethics* 2023, 24(1):49.

[67] Haas MA, Teare H, Prictor M, Ceregra G, Vidgen ME, *et al.* 'CTRL': an online, dynamic consent and participant engagement platform working towards solving the complexities of consent in genomic research. *Eur. J. Hum. Genet.* 2021, 29(4):687–698.

[68] Piasecki S, Chen J. Complying with the GDPR when vulnerable people use smart devices. *Int. Data Priv. Law* 2022, 12(2):113–131.

[69] Mantelero A. Artificial Intelligence and data protection: challenges and possible remedies. 2019. Available: https://www.aepd.es/documento/report-ai.pdf (accessed on 21 November 2025).

[70] Bijker WE. Anchoring innovation as a form of social construction of technology. In *Greco-Roman Studies in Anchoring Innovation*. Boston: Brill, 2025.

[71] Pinch TJ, Bijker WE. The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other. *Soc. Stud. Sci.* 1984, 14(3):399–441.

[72] Adashi EY, Walters LB, Menikoff JA. The Belmont report at 40: reckoning with time. *Am. J. Public Health* 2018, 108(10):1345–1348.

[73] Dankar FK, Gergely M, Dankar SK. Informed consent in biomedical research. *Comput. Struct. Biotechnol. J.* 2019, 17:463–474.

[74] Claerhout B, DeMoor GJ. Privacy protection for clinical and genomic data: the use of privacy-enhancing techniques in medicine. *Int. J. Med. Inform.* 2005, 74(2–4):257–265.

[75] Raisaro JL. Privacy-enhancing technologies for medical and genomic data: from theory to practice. 2018. Available: https://infoscience.epfl.ch/entities/publication/c0177b4f-6a67-42b9-81ed-ee9497bc5535 (accessed on 21 November 2025).