v3: 9 February 2026

Commentary

Trust and Trade: Ethical Reflections on Patient Trust and the Monetisation of Real-World Data

Preprinted: 7 October 2025
Peer-approved: 26 January 2026

Qeios, Vol. 8 (2026)
ISSN: 2632-3834

Alexandros Sagkriotis[1]

1. Independent Consultant in Real-World Evidence and Health Data Science, United Kingdom

Real-world data (RWD) and real-world evidence (RWE) are now central to healthcare decision-making, supporting regulatory submissions, health technology assessments (HTA), and scientific communication. Yet patients whose data fuel these processes rarely see transparency or benefit when their information is commercialised. Governance frameworks from the European Medicines Agency (EMA), U.S. Food and Drug Administration (FDA), and other bodies emphasise methodological rigour and transparency, but they do not directly adjudicate questions of fairness, reciprocity, or perceived legitimacy from a patient perspective, which largely fall outside their formal remits. For clarity of scope, this commentary focuses specifically on patient perceptions of fairness, reciprocity, and legitimacy in the monetisation of secondary-use health data; it does not examine urgency-of-use questions, direct clinical benefits, or broader societal goals of data-driven healthcare.

This article is a normative commentary informed by published patient surveys, governance case studies, and regulatory experience. It does not present original patient research but synthesises recurring patient-relevant concerns regarding trust, fairness, and public value in the secondary use of health data.

This commentary argues that evidence integrity must extend beyond technical standards to encompass ethical stewardship. Drawing on case examples from the UK, EU, and North America, it shows how opacity in consent processes, selective disclosure of data use, and the absence of benefit-sharing widen the trust gap. Patients contribute information under the assumption it will improve care, not simply generate commercial value or institutional advantage.

To address this, five pragmatic safeguards are proposed:

i. transparent, plain-language consent;

ii. mandatory disclosure of monetisation models;

iii. governance boards with patient representation; While many national and international data governance bodies now include patient or public representatives, the depth of their influence varies considerably. In several early national data initiatives, patient involvement was limited to advisory or consultative roles without formal voting rights, agenda-setting authority, or oversight of commercial access decisions. Such structures risk being perceived as symbolic rather than substantive participation, reinforcing concerns about tokenism when representation is not matched by real decision power.

 doi.org/10.32388/RHIP9A.7

iv. reinvestment of commercial gains into patient support, public health, and digital tools; Benefit sharing should not be interpreted as direct financial remuneration to individual patients, which is neither feasible nor desirable in most regulatory and research contexts. Rather, it refers to structured reinvestment of value generated from secondary data use into patient-relevant public goods, such as disease registries, patient organisations (including umbrella and European-level federations for rare diseases), digital infrastructure, education, and support services. In this way, reciprocity is achieved at community and system level, even when data originate from multiple countries and fragmented patient populations.
v. mandatory registration of non-interventional studies in public registries.
Together, these measures extend evidence integrity to include fairness, reciprocity, and legitimacy.
Together, these measures extend evidence integrity to include fairness, reciprocity, and legitimacy.
The future of RWE depends not only on scientific validity but also on whether patients trust that their data are handled responsibly and ethically. Perhaps it is time to move beyond passive consent and towards a new call for accountability—captured in a simple but powerful reminder: *"That is MY DATA."*
This commentary is informed by principles of relational ethics and the *social responsibility of science*, framing data monetisation as both a technical and moral question of reciprocity and legitimacy. These safeguards are grounded in emerging international experience with data transparency and patient governance, though practical challenges and alternative frameworks are discussed.

Corresponding Author: Alexandros Sagkriotis: asagkriotis@gmail.com

Introduction

Real-world data (RWD) are firmly embedded in regulatory science and health policy, with the European Medicines Agency (EMA) and the U.S. Food and Drug Administration (FDA) formally recognising real-world evidence (RWE) as a key element across the product lifecycle [1][2]. The Data Analysis and Real World Interrogation Network in the European Union (DARWIN EU) exemplifies the move from principles to execution by routinely generating regulator-led studies across Europe [3]. Yet these frameworks prioritise methodological adequacy and transparency; they do not meaningfully adjudicate the fairness of monetised secondary use from a patient's point of view.

From a European regulatory perspective, patient representation is already formally embedded in several governance structures. In particular, the EMA's DARWIN EU network includes patient and healthcare professional representatives in its advisory and steering activities, and its studies are conducted under a public-interest, non-commercial model in which data are not sold but made available for regulator-led research and methodological development. Acknowledging such initiatives is important to distinguish publicly governed, solidarity-based data ecosystems from commercial or hybrid secondary-use models, which raise different ethical and legitimacy questions.

Concurrently, the European Health Data Space (EHDS) introduces a legal infrastructure for the primary and secondary use of electronic health data (in

force from 26 March 2025), explicitly enabling reuse for research and policy while strengthening individual control [4]. This represents a pivotal opportunity to align governance with public expectations around trust and benefit-sharing.

This paper does not attempt to re-evaluate the methodological standards already established for RWE. Instead, it asks a more fundamental set of questions:

- How do current regulatory and health technology assessment (HTA) frameworks address—or fail to address—the fairness of secondary use and monetisation of RWD?
- To what extent are patients informed about, and comfortable with, their data being transformed into economic value for institutions, companies, or individual careers?
- What safeguards could strengthen trust, reciprocity, and legitimacy in the secondary use of health data?

The objective is to extend the concept of evidence integrity beyond methodological rigour, arguing that patients' trust and perceptions of fairness must be central to the future credibility of RWE.

From a theoretical standpoint, this paper draws on *relational ethics*—which emphasises reciprocity and interdependence between data contributors and data users—and on the *social responsibility of science*, which situates evidence generation within collective obligations toward public good and democratic participation. To delineate the boundaries of this commentary, the analysis concentrates on ethical and relational dimensions of secondary data monetisation from a patient perspective. It does not address other important themes such as clinical urgency, operational efficiency, or broader societal objectives of data-driven transformation, which, while relevant, fall outside this paper's core ethical focus. These frameworks guide the interpretation of trust, fairness, and legitimacy throughout the paper.

These safeguards are presented as ethical and policy recommendations intended to inform governance design and future regulatory development, rather than as immediately binding legal standards. Their purpose is to guide institutional practice and public accountability while remaining adaptable across jurisdictions.

What current frameworks cover—and what they miss

While the EHDS represents a major regulatory advance, its current implementation trajectory reflects political, institutional, and economic compromises rather than a blank-slate redesign. Early policy signals suggest a continued emphasis on system-level access and secondary use efficiencies, with more limited operationalisation of patients as primary data stewards. Recognising this reality is essential: strengthening trust does not mean abandoning the EHDS but rather identifying where relational and ethical safeguards must be reinforced within its existing architecture.

Before examining governance gaps, it is important to define that the term 'monetisation' in this commentary refers to economic value generation from secondary-use health data by public institutions, private companies, data intermediaries, and technology vendors. For clarity, the terms "commercialisation" and "monetisation" are used interchangeably throughout to denote the generation of financial or strategic value from secondary data use.

In practice, monetisation of secondary-use health data occurs through several mechanisms that remain largely invisible to data contributors:

i. licensing of large-scale de-identified EHR datasets by platform vendors to pharmaceutical, med-tech, and AI companies;
ii. aggregation and resale of longitudinal patient data by data brokers operating across jurisdictions;
iii. use of routine clinical data to train proprietary algorithms and digital biomarkers, where economic value is generated through downstream products rather than direct data access fees.

In most such arrangements, patients are informed neither of the pricing structures nor of the commercial pathways through which value is extracted.

Regulatory and HTA-related guidance has matured rapidly: STaRT-RWE standardises protocol transparency [5]; HARPER provides a harmonised protocol template [6]; and the EUnetHTA REQueST tool articulates registry quality criteria [7]. While regulatory authorities and HTA bodies are not data-governance authorities per se, their evidentiary requirements and methodological frameworks indirectly shape incentives, access models, and practices surrounding the secondary use of real-world data. These instruments sharpen scientific validity and reporting, but they are agnostic about who benefits economically from secondary use and how that is disclosed to patients. In practice, monetisation occurs through several mechanisms: (i) health systems or EHR vendors licensing de-identified datasets; (ii) private data brokers aggregating and selling longitudinal health data; (iii) pharmaceutical and med-tech companies purchasing access for research and evidence generation; and (iv) digital platforms generating value through algorithm development or proprietary analytics.

The FDA's RWE framework and its 2025 programme updates reiterate definitions and decision contexts for using RWD in approvals and labelling changes—again, squarely methodological. The result is a governance landscape that improves science but leaves the ethics of monetisation and reciprocity largely to institutional policies and contracts [2].

The patient trust gap

Survey work in the United Kingdom (UK) consistently shows high trust in the National Health Service (NHS) as a steward of data, but markedly lower trust in pharmaceutical and technology companies. In 2024, NHS Digital reported 72–83% trust in the NHS to keep data secure; curated evidence reviews from Understanding Patient Data (2021–2024) similarly document both broad support for data use and persistent unfamiliarity with secondary uses. Public preference skews towards de-identified data and transparency about purpose [8].

Findings from a 2024 systematic review show that public discomfort with commercial access remains high, especially when data are used for marketing or insurance purposes. The review also highlights that willingness to share for third-party uses hinges on trust, perceived public benefit, and clear safeguards [9]. Earlier UK surveys confirm these trends, with NHS stewardship trusted far more than corporate actors [8]. These findings reinforce the central argument of this commentary: patients distinguish sharply between public-benefit-oriented data use and commercial or opaque models of data value extraction.

Global consumer research echoes this. Deloitte's 2024–2025 surveys find rising scepticism toward generative AI in health contexts, driven by distrust in outputs and unease about data handling—signals that any monetised data ecosystem must take seriously [10].

An often-overlooked precondition for trust is digital health literacy. For many patients—and even for experts—the practical implications of data linkage, secondary use, and data breaches remain opaque. Without a basic understanding of risks, benefits, and safeguards, meaningful risk–benefit assessment is severely constrained. In this context, consent risks becoming procedural rather than substantive: a formal act without informed agency. Ethical governance of secondary data use therefore depends not only on safeguards but also on sustained investment in public digital health literacy.

In many settings, consent risks becoming a procedural checkpoint rather than a genuinely relational dialogue, reinforcing asymmetries of information and control between institutions and patients. Ethical stewardship therefore requires moving beyond formal compliance towards meaningful understanding and reciprocity.

Case illustrations: when opacity erodes legitimacy

While both the DeepMind–Royal Free and NHS data platform debates reveal governance fragility, the DeepMind case illustrates in detail how the absence of early engagement erodes legitimacy. Analysing this case through the lens of *relational ethics* clarifies that the failure was not merely procedural but relational —patients were treated as data sources rather than moral partners.

DeepMind–Royal Free (UK): In 2017, the UK Information Commissioner's Office concluded that the Royal Free NHS Foundation Trust failed to comply with data protection law in sharing 1.6 million patient records with Google's DeepMind to develop and test the Streams app, citing inadequate patient information. The episode is now a canonical example of "legal-process first, engagement later" and its reputational cost [11].

Although this case predates the COVID-19 pandemic and the current wave of generative-AI applications, it remains one of the few large-scale health-data partnerships to have been fully examined by an independent regulator and documented in a legally reasoned public decision. Many more recent collaborations operate under complex contractual arrangements and non-disclosure agreements and have not yet been subject to comparable public adjudication, which is why DeepMind–Royal Free continues to serve as the most transparent and instructive reference case.

NHS national data platform and pricing debates: In parallel with NHS England's Federated Data Platform build-out, policy discussions have explored a national health data service and pricing structures to recover the costs of access. Editorials warn that perceived private profit from NHS data could undermine trust without visible public benefit and transparency [12].

Both cases illustrate what happens when public data are treated primarily as assets rather than as contributions from individuals—people who may rightfully feel, 'this is my data,' yet are rarely consulted on its use.

Legal and Ethical Governance of Secondary Data Use in the UK

In the UK, the secondary use of health data operates within a well-established legal and ethical governance framework. Under UK GDPR, secondary use requires an appropriate lawful basis, which does not necessarily rely on individual consent. For certain non-interventional research uses of confidential patient information where consent is impracticable, Section 251 support may be granted under the NHS Act 2006.

This support is overseen by the Health Research Authority's Confidentiality Advisory Group (CAG), which includes lay representation to ensure public perspectives are considered. CAG approvals are conditional on transparency notices, clear opt-out mechanisms, ongoing Patient and Public Involvement and Engagement (PPIE), annual reporting, and incident-reporting obligations.

This framework illustrates that, at least in the UK, the secondary use of patient data is subject to robust governance rather than a regulatory vacuum.

Monetisation: ethics and economics

Health systems, electronic health record (EHR) vendors, and third-party platforms increasingly treat de-identified data as an asset class. Recent scholarship documents data collection and commercialisation practices in primary care record industries, and ethics papers debate whether and when for-profit secondary use of publicly generated data is acceptable. Publics tend to support research-oriented reuse with clear public benefit but react negatively to opaque commercial models [13]. This commentary uses 'commercialisation' and 'monetisation' to denote value flows—financial or strategic—generated from patient data, regardless of whether value accrues to public bodies, private companies, or hybrid partnerships.

It is important to distinguish between profit-seeking monetisation and legitimate cost-recovery. Data curation, secure infrastructure, governance oversight, metadata preparation, archiving, and compliance with legal and ethical requirements entail substantial and ongoing costs. In many cases, data access fees are designed to recover these costs rather than to generate surplus profit.

Public value derived from data reuse should therefore be understood broadly—not only in financial terms but also through population-level health benefits, safety monitoring, system learning, and improved care delivery.

In the UK, British Medical Journal (BMJ) commentary has cautioned against "selling NHS patient data" without clear benefit-sharing and transparent governance—again reflecting a legitimacy rather than a pure privacy concern [14]. The National Data Guardian's 2023–24 report similarly centres "demonstrably trustworthy" use as essential to public confidence [15].

Viewed through *social responsibility ethics*, the monetisation of health data raises questions not of ownership alone but of distributive justice—who benefits, and who bears the moral cost of data extraction.

From method to meaning: expanding "evidence integrity"

Scientific transparency tools (STaRT-RWE, HARPER, REQueST) should be complemented by trust-building practices that speak to meaning for contributors: who profits, who governs, and who benefits. Absent this, even lawful, de-identified reuse may fail the legitimacy test—especially at scale or when private actors are central [16]. Further discussion of secondary use under the European Health Data Space (EHDS) and privacy-enhancing technologies is provided by van Drumpt et al. [17].

Five pragmatic safeguards

Building on the legitimacy principles outlined above, the following five safeguards operationalise *relational ethics* and the *social responsibility of science* in practice. They translate fairness, reciprocity, and accountability into concrete governance mechanisms that extend beyond compliance. These safeguards are designed to address patient-centred legitimacy concerns specifically in contexts where data generate economic value for institutions or companies; they do not aim to regulate clinical care use or direct public-health emergencies.

These safeguards should be understood as pragmatic starting points for policy discussion and iterative refinement, rather than definitive or universally prescriptive solutions, recognising the practical, legal, and operational constraints faced by data ecosystems.

1. **Plain-language, layered consent (or notification) for secondary uses.** Consent materials should explain what kinds of secondary use and monetisation exist, by whom, and with what controls, aligned to EHDS guardrails and national opt-out regimes [4].
2. **Mandatory disclosure of monetisation models.** Public registries of data access agreements (who accessed, for what, value exchanged) would normalise transparency and enable audit—akin to trial registration for methods [18].
3. **Governance with patient representation.** Data access boards for secondary use should include trained patient/public members with real voting rights. This is consistent with the National Data Guardian's emphasis on "demonstrably trustworthy" use [15].
4. **Visible benefit-sharing.** Where commercial value is created from public data, a defined proportion should be reinvested into patient support, patient associations, public health, digital tools, or the data infrastructure itself. Ongoing UK work on pricing/cost-recovery shows how models can be designed to avoid perceptions of "selling" while still covering costs [12].
5. **Protocol registration and transparency.** All non-interventional studies using patient data—whether for HTA, regulatory submissions, or scientific communication—should be registered in publicly accessible databases such as the EU PAS Register, ClinicalTrials.gov, or ENCePP [19][20][21]. Registration of objectives, endpoints, and analysis plans creates a transparent record that reduces selective reporting, clarifies intent, and enhances accountability. This expectation should extend to both submission-grade and non-submission RWE, ensuring that the use of patient data is always

visible and auditable [22][23]. Registration promotes transparency and accountability but does not constitute regulatory approval.

Together, these steps do not supplant methodological standards; they expand the meaning of "evidence integrity" to include fairness, reciprocity, and legitimacy—anchoring ethical trust as a measurable dimension of scientific quality.

Legitimate secondary uses

Access by industry to patient-level data for purposes such as HTA submissions, regulatory evidence generation, and peer-reviewed scientific communication should be regarded as legitimate and essential. For pharmaceutical manufacturers, access to unbiased real-world data is not optional but central to fulfilling post-authorisation safety and effectiveness obligations. These activities contribute to transparency in decision-making, accelerate patient access to innovative therapies, and improve clinical practice.

However, legitimacy requires that such uses are conducted within the same framework of safeguards: plain-language consent, disclosure of access agreements, patient-inclusive governance, visible benefit-sharing, and mandatory registration of protocols in publicly accessible registries such as the EU PAS Register, ClinicalTrials.gov, or ENCePP. Without these guardrails, even necessary evidence generation risks being perceived as exploitation rather than collaboration.

These legitimate uses set the ethical boundary conditions for the five safeguards proposed below.

Discussion

The analysis presented here highlights a structural blind spot in the governance of RWE. Regulatory and HTA frameworks have succeeded in advancing methodological rigour, transparency, and data quality, but they remain silent on fairness, reciprocity, and benefit-sharing. The ethical challenges discussed here apply primarily to commercial and hybrid data ecosystems; publicly governed, regulator-led infrastructures such as DARWIN EU or ENCePP already embody many of the proposed safeguards through non-profit access models, public accountability, and formal patient involvement.

This commentary does not claim to represent the full spectrum of patient perspectives across all health systems. Rather, it synthesises recurring themes from surveys, qualitative studies, and high-profile governance cases to illustrate how the trust gap manifests across settings. Surveys and case studies show that while patients broadly support data use for public benefit, they are consistently uneasy about opaque commercial access and monetisation. This trust gap poses a risk not only to the legitimacy of individual initiatives but to the credibility of RWE as a scientific field.

It is equally important to recognise the countervailing ethical argument: that failure to share anonymised or pseudonymised health data may itself be unethical when it impedes learning, perpetuates inequity of access, or delays improvements in quality of care. From this perspective, data non-use and over-restriction can harm patients just as surely as misuse. The position advanced in this commentary is therefore not anti–data sharing, but pro–legitimate sharing: data reuse, including by commercial and regulatory actors, is both necessary and

desirable, provided it is conducted within transparent, reciprocal, and patient-inclusive governance frameworks that preserve trust and social value.

Within the European Health Data Space (EHDS), these safeguards could be operationalised through existing governance structures rather than parallel mechanisms. Health Data Access Bodies could host public registries of secondary-use agreements and oversee patient-representative voting on access decisions. Cost-recovery and pricing frameworks offer natural vehicles for structured reinvestment of value into patient and public goods, while protocol registration could be embedded as a precondition for secondary-use permits. In this way, ethical reciprocity can be integrated directly into the emerging EHDS architecture.

In the UK context, this debate must also be situated within the reciprocal social contract articulated in the NHS Constitution. While the NHS pledges to protect confidentiality and anonymise data, it also commits to using patient information to support research and improve care for others. In this sense, data contribution reflects a form of civic altruism underpinning evidence-based healthcare.

Erosion of trust risks undermining this social licence, as evidenced by rising national opt-out rates. If public confidence is weakened through imprecise narratives around data use and monetisation, the integrity and representativeness of real-world evidence itself may be compromised.

At its core, this blind spot reflects a tension between methodological integrity—how well evidence is generated—and relational integrity—how fairly data relationships are governed. *Relational ethics* provides a lens through which this imbalance can be addressed. It frames patients not as passive data sources but as moral agents who participate in a continuous exchange of trust, expectation, and accountability. From this perspective, transparency is not a bureaucratic checkbox but an act of recognition and respect, and consent becomes an ongoing dialogue rather than a one-time procedural formality.

The DeepMind–Royal Free case serves as a vivid example of what happens when these relational dimensions are ignored. Despite legal authorisation, the absence of patient engagement created a perception of data extraction rather than partnership. Reinterpreting such cases through *relational ethics* suggests that failures in public confidence are rarely technical—they are relational, arising when institutions treat data ownership as property instead of stewardship. Rebuilding this moral relationship requires new norms of dialogue, reciprocity, and visible accountability.

The *social responsibility of science* extends this reasoning from the interpersonal to the societal level. Scientific and commercial actors alike benefit from a social licence granted by citizens who share data in good faith. That licence carries duties: to reinvest value into patient communities, to democratise access to insights derived from shared data, and to ensure that monetisation does not become exploitation. Reinvestment in public infrastructure, open methods, and digital literacy programmes are therefore not peripheral acts of goodwill but expressions of moral reciprocity [24][25]. The proposed safeguards operationalise these duties in practical terms.

The safeguards proposed—transparent consent, disclosure of monetisation, patient representation in governance, visible benefit-sharing, and mandatory protocol registration—are not aspirational ideals but practical steps already mirrored in related domains, from trial registration to public involvement in research ethics. Each safeguard reflects a dimension of relational or social ethics

in action: plain-language consent fosters informed participation; disclosure of monetisation makes visible the economic flows underpinning evidence generation; governance with patient representation redistributes epistemic authority; visible benefit-sharing acknowledges the collective origins of data value; and protocol registration transforms accountability into a traceable public record. Together, these measures link ethical theory to institutional design.

Critical Appraisal of the Five Safeguards: Strengths, Constraints, and Alternatives.

These safeguards are proposed with full recognition that they operate within existing legal, technical, and political constraints, and that no single measure can fully resolve legitimacy deficits without broader cultural and educational change.

While the five safeguards proposed in this commentary are pragmatic extensions of relational and social ethics, their implementation is not without challenges. Transparent consent may face practical limits when secondary uses are numerous or evolving; layered consent models tested in the UK's care.data and NHS app frameworks show both feasibility and fatigue. Mandatory disclosure of monetisation models can encounter proprietary-data constraints, though pilot registries (e.g., Health Data Research UK's Innovation Gateway) demonstrate that summary-level transparency is achievable. Patient representation in governance requires training and institutional support to avoid tokenism, as seen in early NHS data board pilots. Reinvestment mechanisms face definitional and administrative hurdles regarding the "fair value" of data, though international experience (e.g., Canada Health Infoway, France's Health Data Hub) illustrates models for reinvestment without direct remuneration. Finally, mandatory registration of non-interventional studies may increase administrative burden, yet parallels with clinical trial registration show that transparency gains outweigh compliance costs.

Inevitably, the implementation of these safeguards will increase administrative burden, require additional legal review, complicate contracting arrangements, raise operational costs, and extend study start-up and data-access timelines.

These additional layers of governance may also raise concerns about participant burden and potential attrition, particularly if consent processes, transparency requirements, and oversight mechanisms are perceived as complex or intrusive. However, experience from national opt-out schemes and public attitude surveys suggests that loss of trust, rather than administrative friction, is the primary driver of disengagement. In this sense, the proposed safeguards should be viewed as protective of long-term participation and data representativeness: by strengthening legitimacy and social licence, they reduce the risk of widespread opt-out, selection bias, and erosion of the evidentiary base. The short-term cost of increased procedural rigour is therefore balanced against the long-term sustainability of real-world data ecosystems.

Disclosure of monetisation models may challenge commercial confidentiality; patient representation in governance requires training and sustained institutional support; benefit-sharing and public registries demand new financial and reporting infrastructures. However, the long-term costs of eroded trust are likely to be far greater. Loss of public confidence translates into rising opt-out rates, reduced representativeness of real-world datasets, reputational damage to institutions and sponsors, and, ultimately, heightened regulatory scrutiny and policy backlash. In this light, the proposed safeguards should be viewed not as bureaucratic overhead, but as investments in the social licence of real-world evidence—protecting the legitimacy, sustainability, and future

usability of patient data, even at the expense of slower and more resource-intensive processes in the short term.

Alternative models—such as dynamic consent, data cooperatives, or public-private data trusts—offer complementary mechanisms to enhance accountability but remain less standardised or scalable across jurisdictions. The five safeguards proposed here were therefore prioritised for their cross-jurisdictional feasibility, institutional maturity, and immediate applicability within existing EMA/FDA/HTA frameworks.

Beyond formal governance, legitimacy also depends on narrative coherence—the stories institutions tell about why and how data are used. Public trust is sustained not only by compliance but by shared meaning. When narratives emphasise partnership, reciprocity, and societal value, they generate alignment; when they focus narrowly on efficiency or profit, they breed scepticism. Embedding narrative transparency into institutional communication—through patient-facing dashboards, co-created public reports, or community advisory panels—can transform technical openness into moral credibility [26][27].

The EHDS now offers a historic opportunity to embed these relational and social dimensions at scale. By linking cross-border health data, the EHDS can enable transformative public health insights, but without deliberate attention to fairness and reciprocity, it risks amplifying the very inequities it seeks to overcome. The success of the EHDS will therefore hinge on whether its implementation includes patient representation in governance boards, clarity around data valuation, and reinvestment mechanisms that channel benefits back to citizens.

Embedding these five safeguards into RWE practice would extend the concept of evidence integrity from methodological adequacy to social legitimacy. This reframing redefines "high-quality evidence" as data that are not only accurate and reproducible but also ethically sourced, transparently governed, and socially reciprocated. In that sense, RWE's future credibility will depend as much on the fairness of its data relationships as on the rigour of its statistics. Only by uniting these two dimensions—scientific validity and moral legitimacy—can the promise of real-world data be realised in full.

Although many examples in this commentary are drawn from the UK and EU, the ethical principles of reciprocity, legitimacy, and benefit-sharing are not jurisdiction-specific. In low- and middle-income countries or mixed public–private systems, similar concerns may arise—often amplified by weaker governance capacity. The safeguards proposed here should therefore be interpreted as adaptable principles rather than region-specific prescriptions.

Conclusion

RWE cannot thrive on methodological excellence alone. Nor can it thrive if ethically justified data reuse is paralysed by mistrust; sustainable evidence generation requires both robust sharing and robust legitimacy. Patients' willingness to share—and society's mandate to use—rests on trust that secondary uses (including monetised ones) are transparent, fairly governed, and deliver visible public benefit. With the EHDS now in force and global transparency tools maturing, the moment is ripe to embed reciprocity into the RWE ecosystem.

The five safeguards outlined in this commentary—plain-language consent, disclosure of monetisation models, governance with patient representation,

visible benefit-sharing, and mandatory protocol registration—provide a feasible framework to achieve this.

While this commentary focuses on ethical legitimacy rather than methodological or operational considerations, future work should integrate these dimensions into a more holistic model of a trustworthy data ecosystem.

Fair governance of real-world data is therefore not merely a regulatory aspiration but a moral contract grounded in *relational ethics* and the *social responsibility of science*. As data ecosystems grow more interconnected, the legitimacy of RWE will depend as much on relational integrity as on analytical precision. Building mechanisms for dialogue, transparency, and visible benefit-sharing can convert data contribution from an act of compliance into one of trust and shared purpose.

The future of RWE will ultimately be measured not only by the robustness of its methods but also by the fairness of its relationships—with patients, with publics, and with the systems that rely on their information.

Perhaps it is time to move beyond passive consent and towards a new call for accountability—one that could be captured in a simple but powerful reminder—used here as a narrative device to reflect patient sentiment—"That is MY DATA."

Future research should empirically test the feasibility and acceptability of these safeguards through pilot RWE programmes under the EHDS and comparable national frameworks, ensuring that ethical principles evolve alongside scientific progress.

Statements and Declarations

Funding

No specific funding was received for this work.

Potential Competing Interests

No potential competing interests to declare. The views expressed are those of the author and do not necessarily reflect the positions of past or current affiliations.

Ethics

This commentary did not involve primary data collection or access to individual-level patient data. All real-world data studies cited were conducted under their respective ethical and legal approvals as reported in the original sources.

Data Availability

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Author Contributions

A.S. is the sole author of this policy brief and is responsible for conceptualisation, drafting, and final approval of the manuscript.

Acknowledgements

The author wishes to thank his daughter for her encouragement and inspiration, which have been a constant reminder of the importance of striving for a fairer

and more evidence-informed healthcare future. With over 30 years of experience in senior leadership roles across global pharmaceutical companies—spanning clinical development, real-world evidence, and medical affairs—the author has drawn on both professional expertise and personal reflections to write this commentary. Portions of the manuscript, including language refinement and structural suggestions, were supported using OpenAI's ChatGPT-5 model. The author critically reviewed, edited, and validated all content to ensure accuracy, originality, and alignment with scholarly standards.

The author gratefully acknowledges the anonymous reviewers for their constructive and thoughtful feedback. Their comments helped refine the conceptual framing, clarify the scope, and strengthen the overall coherence of this commentary. The revisions incorporated have meaningfully improved the manuscript and enhanced its contribution to the ongoing debate on the ethical stewardship of real-world data.

The author is affiliated with Helios Academy Limited | Where Science Meets Compassion, an educational and scientific initiative devoted to transparent evidence generation and ethical leadership in healthcare. This commentary reflects the author's independent scholarly perspective and commitment to advancing the trustworthy and patient-centred use of real-world data.

References

1. ^*European Medicines Agency (2025). "Real-World Evidence." EMA. https://www.ema.europa.eu/en/about-us/how-we-work/data-regulation-big-data-other-sources/real-world-evidence.*
2. a, b*U.S. Food and Drug Administration (2018). "Framework for FDAs Real-World Evidence Program." FDA. https://www.fda.gov/media/120060/download.*
3. ^*DARWIN EU (2025). "About DARWIN EU." DARWIN EU. https://www.darwin-eu.org/.*
4. a, b*European Commission, Council of the European Union (2025). "European Health Data Space Regulation (EHDS)." European Commission. https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en.*
5. ^*Wang S, Pinheiro S, Hua W, Arlett P, Uyama Y, Berlin J, Bartels D, Kahler K, Bessette L, Schneeweiss S (2021). "STaRT-RWE: Structured Template for Planning and Reporting on the Implementation of Real World Evidence Studies." BMJ. m4856. doi:10.1136/bmj.m4856.*
6. ^*Wang S, Pottegrd A, Crown W, Arlett P, Ashcroft D, Benchimol E, Berger M, Crane G, Goettsch W, Hua W, Kabadi S, Kern D, Kurz X, Langan S, Nonaka T, Orsini L, PerezGutthann S, Pinheiro S, Pratt N, Schneeweiss S, Toussi M, Williams R (2022). "HARmonized Protocol Template to Enhance Reproducibility of Hypothesis Evaluating RealWorld Evidence Studies on Treatment Effects: A Good Practices Report of a Joint ISPE/ISPOR Task Force." Pharmacoepidemiol Drug Saf. **32**(1):4455. doi:10.1002/pds.5507.*
7. ^*European Network for Health Technology Assessment (EUnetHTA) (2023). "Registry Evaluation and Quality Standards Tool (REQueST)." European Medicines Agency catalogues. https://catalogues.ema.europa.eu/system/files/2025-02/05.01.0301%20Feasibility%20Documentation%20%20-%20Registry%20Evaluation%20and%20Quality%20Standards%20Tool%20%28REQueST%29%20_%2010-Sep-2023 Redacted.pdf.*

8. ^a, ^b*NHS England, NHS Digital (2024). "Public Attitudes to Data in the NHS and Social Care." NHS Digital. https://digital.nhs.uk/data-and-information/keeping-data-safe-and-benefitting-the-public/public-attitudes-to-data-in-the-nhs-and-social-care.*
9. ^*Ipsos MORI (2017). "The One-Way Mirror: Public Attitudes to Commercial Access to Health Data." Wellcome Trust. doi:10.6084/m9.figshare.5616448.v1.*
10. ^*Deloitte Insights (2024). "Consumer Trust in Healthcare Generative AI (2024) and 2025 Global Healthcare Outlook." Deloitte Insights. https://www.deloitte.com/us/en/insights/industry/health-care/consumer-trust-in-health-care-generative-ai.html.*
11. ^*ICO (UK) (2017). "DeepMind and Royal Free Case Resources (Patient Data Sharing Ruling)." National Health Executive. https://www.nationalhealthexecutive.com/Research-and-Technology/patient-data-transfer-to-google-deepmind-by-trust-deemed-unlawful-by-ico.*
12. ^a, ^b*Financial Times (2024). "UK Studies Pricing Plan for Selling NHS Patient Data." Financial Times. https://www.ft.com/content/9ec787a8-60d5-4899-8223-81335dfa919b.*
13. ^*Spithoff S, Vesely L, McPhail B, Rowe R, Mogic L, Grundy Q (2025). "The Primary Care Medical Record Industry in Canada and Its Data Collection and Commercialization Practices." JAMA Netw Open. **8**(5):e257688. doi:10.1001/jamanetworkopen.2025.7688.*
14. ^*Morley J, Hamilton N, Floridi L (2024). "Selling NHS Patient Data." BMJ. q420. doi:10.1136/bmj.q420.*
15. ^a, ^b*National Data Guardian (UK) (2024). "Annual Report 20232024." Department of Health and Social Care. https://www.gov.uk/government/publications/national-data-guardian-2023-2024-report/national-data-guardian-2023-2024-report.*
16. ^*Guilhaume C (2021). "A Tool to Assess the Registries Quality: The Registry Evaluation and Quality Standards Tool (REQueST)." Eur J Public Health. **31**(Supplement_3). doi:10.1093/eurpub/ckab164.573.*
17. ^*van Drumpt S, Chawla K, Barbereau T, Spagnuelo D, van de Burgwal L (2025). "Secondary Use Under the European Health Data Space: Setting the Scene and Towards a Research Agenda on Privacy-Enhancing Technologies." Front Digit Health. **7**. doi:10.3389/fdgth.2025.1602101.*
18. ^*International Society for Pharmacoeconomics and Outcomes Research (ISPOR), International Society for Pharmacoepidemiology (ISPE), Duke-Margolis Center for Health Policy, National Pharmaceutical Council (NPC) (2020). "Real-World Evidence Transparency Initiative." ISPOR. https://www.ispor.org/strategic-initiatives/real-world-evidence/real-world-evidence-transparency-initiative.*
19. ^*European Medicines Agency (2025). "ENCePP: European Network of Centres for Pharmacoepidemiology and Pharmacovigilance." EMA. https://www.encepp.eu/.*
20. ^*European Medicines Agency (2025). "EU PAS Register: European Union Electronic Register of Post-Authorisation Studies." EMA. https://www.encepp.eu/encepp/studiesDatabase.jsp.*
21. ^*U.S. National Library of Medicine (2025). "ClinicalTrials.gov." National Institutes of Health. https://clinicaltrials.gov/.*
22. ^*Naudet F, Patel C, DeVito N, Le Goff G, Cristea I, Braillon A, Hoffmann S (2024). "Improving the Transparency and Reliability of Observational Studies Through Registration." BMJ. e076123. doi:10.1136/bmj-2023-076123.*
23. ^*Council of the European Union (2025). "European Health Data Space: Council Adopts New Regulation Improving Cross-Border Access to EU Health Data." Counci*

l of the EU. https://www.consilium.europa.eu/en/press/press-releases/2025/01/21/european-health-data-space-council-adopts-new-regulation-improving-cross-border-access-to-eu-health-data/.

24. ^*Shaw E (2011). "Relational Ethics and Moral Imagination in Contemporary Systemic Practice." Aust N Z J Fam Ther.* **32**(1):114. doi:10.1375/anft.32.1.1.
25. ^*Resnik D, Elliott K (2016). "The Ethical Challenges of Socially Responsible Science." Account Res.* **23**(1):3146. doi:10.1080/08989621.2014.1002608.
26. ^*Floridi L, Taddeo M (2016). "What Is Data Ethics?" Philos Trans A Math Phys Eng Sci.* **374**(2083):20160360. doi:10.1098/rsta.2016.0360.
27. ^*Carter P, Laurie G, Dixon-Woods M (2015). "The Social Licence for Research: Why Care.Data Ran Into Trouble." J Med Ethics.* **41**(5):404409. doi:10.1136/medethics-2014-102374.

Declarations

Funding: No specific funding was received for this work.
Potential competing interests: No potential competing interests to declare.