laws

MDPI

Review

Beyond Consent-Centred Protection in Digital Healthcare: Italy, Secondary Use of Health Data, and Governance-Based Safeguards for AI-Mediated Care

Tommaso Spasari [1], Paolo Bailo [2], Giuliano Pesel [2], Giovanni D'Alessandro [3,*] and Giovanna Ricci [2]

[1] Section of Occupational and Legal Medicine and BioLaw, University Niccolò Cusano, 00166 Rome, Italy; tommaso.spasari@unicusano.it
[2] Section of Legal Medicine, School of Law, University of Camerino, 62032 Camerino, Italy; paolo.bailo@unicam.it (P.B.); dr.giuliano.pesel@gmail.com (G.P.); giovanna.ricci@unicam.it (G.R.)
[3] Department of Political, Legal, Sociological and Humanistic Sciences, University Niccolò Cusano, 00166 Rome, Italy
* Correspondence: giovanni.dalessandro@unicusano.it

Abstract

The digitalisation of healthcare is transforming not only clinical practice but also the legal architecture through which health rights are protected, coordinated, and operationalised. Using Italy as a doctrinal case study within the European Union (EU) framework shaped by the General Data Protection Regulation, the European Health Data Space, and artificial intelligence (AI) regulation, this article argues that digital healthcare is moving beyond consent-centred protection toward governance-based safeguards. The Italian trajectory is especially revealing because regionalised healthcare governance intersects with centralised digital coordination through the Fascicolo Sanitario Elettronico, the Ecosystem of Health Data, and EU rules on the secondary use of health data. The article contends that this shift does not displace consent as a legal or constitutional value, but requires stronger substitute and complementary safeguards when consent can no longer operate as an effective practical control mechanism. These include clear legal bases, differentiated access regimes, data minimisation, secure processing environments, meaningful patient information, democratic accountability, human oversight, anti-discrimination duties, and clearer allocations of responsibility among clinicians, institutions, and technology providers. AI-mediated care is treated as a downstream test case for whether governance-based legality remains compatible with autonomy, dignity, and responsibility in clinical care.

Keywords: digital health; health data governance; patient autonomy; secondary use of health data; electronic health record; European Health Data Space; artificial intelligence in healthcare; informed consent; human oversight; medical liability

Academic Editor: Aisling De Paor

Received: 20 April 2026
Revised: 4 July 2026
Accepted: 14 July 2026
Published: 21 July 2026

1. Introduction

The digitalisation of healthcare is one of the most consequential legal transformations in contemporary medicine. Artificial intelligence (AI), interoperable health-information infrastructures, remote monitoring, and data-intensive models of care are no longer peripheral innovations; they increasingly structure ordinary prevention, diagnosis, treatment, and long-term management. Their juridical significance lies not only in efficiency or predictive capacity, but in the way digital environments reshape the conditions under which health rights are exercised, protected, and limited (Schwab 2016; Topol 2019; Nittari et al.

2020). The central issue is therefore not simply whether digital tools improve medicine, but how the law should regulate the infrastructures, institutional powers, and accountability arrangements through which digital care is made possible (World Health Organization 2021; European Parliament and Council 2016).

Health data occupy a singular place in that transformation. They are indispensable to continuity of care, public-health planning, scientific research, and the operation of data-driven health systems, yet they also concern the most intimate dimensions of bodily and mental integrity and therefore attract heightened legal protection (European Parliament and Council 2016; European Court of Human Rights 2014). For that reason, the legal problem can no longer be reduced to the confidentiality of isolated data-processing operations. Contemporary healthcare increasingly relies on complex informational ecosystems in which data are generated, combined, reused, and interpreted across multiple institutional settings. In that environment, privacy remains essential, but it is no longer sufficient as the sole conceptual lens; the centre of gravity shifts from the policing of discrete processing acts to the governance of infrastructures, access conditions, reuse mechanisms, and decision-support environments (Slokenberga et al. 2025; Quinn et al. 2024; Becker et al. 2022).

The Italian case is particularly useful for analysing that shift. Constitutional protection of health under Article 32 has always required a balance between the individual dimension of care and the collective interest in public health (Italy 1948). At the same time, the Italian health system remains shaped by the post-Title V tension between national coordination and regional autonomy. Title V refers to Title V of Part II of the Italian Constitution, whose 2001 reform reshaped the allocation of legislative competences between the State and the Regions. That distinction is important in digital health because healthcare organisations remain regionally embedded, while interoperability, essential levels of care, national health-information systems, and statistical or digital coordination require increasingly dense national steering (Italy 1948, 2001; Constitutional Court of Italy 2002). Italy thus offers more than a local example: it is a doctrinally revealing setting in which to observe how constitutional health protection, regional autonomy, national coordination, and European data governance are being recomposed within a single legal architecture (Presidenza del Consiglio dei Ministri 2021; Murgia et al. 2025).

That national trajectory now intersects with a broader European Union (EU) transition. Regulation (EU) 2025/327 establishes the European Health Data Space (EHDS) as a sector-specific data space for primary and secondary uses of electronic health data, while the AI Act and the Italian Law No. 132/2025 progressively structure the legal environment for AI-mediated healthcare (European Parliament and Council 2025, 2024b; Italy 2025). The resulting problem is not merely technical. It concerns the changing basis on which law legitimises the use of health data and the use of algorithmic outputs in care. Consent remains important, but its role is increasingly differentiated and context-dependent: General Data Protection Regulation (GDPR) consent, consent to treatment, and autonomy as a broader constitutional value can no longer be treated as interchangeable concepts (Italy 2017b; Borg and Caruana 2024; Hjort 2025).

This article argues that the legal legitimacy of digital healthcare is moving beyond consent-centred protection rather than from consent to governance in a mutually exclusive sense. Consent remains important, but its role is increasingly differentiated and context-dependent. In large-scale health-data ecosystems, episodic and transaction-specific consent often cannot perform the whole protective function traditionally attributed to it. The relevant question is therefore when alternative legal bases, public-law authorisations, and institutional governance mechanisms may compensate for the reduced practical centrality of consent while preserving autonomy, dignity, equality, and clinically meaningful human responsibility (Rak 2024; Kaltenbrunner 2026; Kumar et al. 2025).

For the purposes of this article, governance-based legality denotes the legal architecture through which digital healthcare is made lawful and normatively defensible by the combined operation of legal bases, special-category conditions, purpose limitation, differentiated access regimes, secure processing environments, data minimisation, auditability, independent supervision, ethics review where relevant, health data access bodies, residual individual rights, meaningful patient information, human oversight, anti-discrimination safeguards, and an intelligible allocation of responsibility. It is not a synonym for administrative convenience or technological coordination. It is a structured legal framework that performs part of the protective work that consent cannot always realistically perform by itself.

The shift also has a democratic dimension. Where individual consent is not the principal control mechanism, institutional decision-making must be justified through democratically enacted legal bases, transparent definitions of public interest, reviewable procedures, independent supervisory authorities, ethics committees or health data access bodies, administrative or judicial remedies, public accountability, and mechanisms that allow affected persons to understand, contest, or limit certain uses of their data. Governance-based legality is therefore legitimate only if it remains anchored in public law, accountability, and contestability rather than in abstract appeals to efficiency or innovation.

2. Method and Analytical Frame

This article adopts a doctrinal legal method centred on the systematic interpretation of the legal framework governing digital healthcare, the secondary use of health data, and AI-assisted clinical decision-making. Primary weight is given to the Constitution of the Italian Republic, European regulations and directives, Italian statutes and decrees, and the opinions and measures of the Italian Data Protection Authority (Garante per la protezione dei dati personali; hereafter, the Italian DPA). Secondary literature is used selectively, not exhaustively, to clarify the specific legal tensions at stake. Italy is treated as a case study because the interaction between regionalised healthcare governance, the evolution of the Italian Fascicolo Sanitario Elettronico (FSE), the Ecosystem of Health Data (EDS), the EHDS, and the recent Italian health-specific AI provisions makes especially visible the movement beyond individual authorisation toward governance-based legality. The article does not assess the technical performance of specific AI systems and does not provide a full comparative survey of all Member States. Its aim is narrower and more legal: to identify the conditions under which public-law coordination, data-protection safeguards, and clinically meaningful responsibility can lawfully complement and compensate for the declining practical centrality of consent in digital healthcare.

3. Italy as a Constitutional and Institutional Case Study

The digital transformation of healthcare in Italy cannot be understood without first recalling that health enjoys a constitutionally privileged status. Article 32 protects health both as an individual fundamental right and as a collective interest, and that duality has always required a balance between personal freedom, public organisation, and institutional responsibility (Italy 1948). In the digital environment, however, that balance is mediated less through isolated clinical acts and more through infrastructures capable of ensuring continuity of care, standardised information flows, and large-scale organisational coordination. The constitutional question is therefore no longer only how the State guarantees access to care, but also how it designs and governs the informational environment through which care is delivered (European Court of Human Rights 2014; Bologna et al. 2016).

This development has direct implications for the balance between the State and the Regions. Title V of Part II of the Italian Constitution, as amended by Constitutional Law No. 3/2001, redefined the distribution of legislative competences between national and

regional institutions. Health protection falls within concurrent legislative competence: the State lays down fundamental principles and guarantees essential levels of care, while Regions retain broad responsibility for healthcare organisation and delivery (Italy 1948, 2001). At the same time, the State retains competences that become especially important in the digital environment, including informational, statistical, and digital coordination and the definition of nationwide interoperability requirements. In the analogue era, regional differentiation could coexist with a relatively fragmented organisational landscape. In the digital era, by contrast, common standards, data continuity, FSE interoperability, and the EDS create centripetal pressure toward national coordination. Digital health does not abolish regional autonomy, but it subjects it to denser requirements of compatibility, legibility, and infrastructural integration (Constitutional Court of Italy 2002; Presidenza del Consiglio dei Ministri 2021).

The FSE is the clearest institutional expression of that shift. Initially framed as a tool to improve continuity of care and access to clinically relevant information, it progressively evolved into a legal and infrastructural device through which the healthcare system becomes more standardised, interoperable, and governable through data (Bologna et al. 2016; Italy 2012a, 2012b). The movement from a more voluntaristic model toward increasingly automatic and interoperable data flows is legally significant because it marks a partial displacement of informational self-determination by public-interest rationales linked to system efficiency, continuity of care, and health-system planning. What was once presented primarily as a patient-facing digital record increasingly functions as a default infrastructure of governance (Italy 2023; Italian Data Protection Authority 2023).

That tendency became even more visible with the reform trajectory surrounding FSE 2.0 (updated Italian electronic health record framework), the EDS, and the 2024 amendments to the Privacy Code introduced in the Italian National Recovery and Resilience Plan (Piano Nazionale di Ripresa e Resilienza) framework. Law No. 56/2024 strengthened the possibility of interconnecting pseudonymised health-information systems at national level and expressly contemplated secure processing environments for anonymous or pseudonymised data, thereby reinforcing the legal relevance of architecture-level safeguards rather than transaction-by-transaction consent (Italy 2024b). The interministerial framework on FSE 2.0 and the subsequent debate on the EDS further confirm that Italian digital-health governance increasingly depends on institutionally designed flows of access, interoperability, and differentiated visibility rather than on isolated manifestations of will (Italy 2023, 2024a; Italian Data Protection Authority 2024a).

In that setting, the role of the Italian DPA is doctrinally central. As the national supervisory authority for personal data protection, the Italian DPA does not merely react to digital-health reforms after their political adoption. Its opinions and corrective interventions help define the legal conditions under which centralised health-data environments may operate. The Authority's importance lies not in rhetorical opposition to innovation, but in its function as an institutional actor shaping safeguards on access, proportionality, data concentration, transparency, and security. The 2024 opinion on the EDS explicitly connected the lawfulness of the new architecture to prior corrections of the FSE 2.0 framework and to the adoption of stronger guarantees against indiscriminate concentration of data (Italian Data Protection Authority 2024a, 2024b). The 2025 follow-up opinion on amendments to the EDS decree confirms that the Authority's interventions are not marginal procedural steps but part of the legal design that shapes centralised health-data governance itself (Italian Data Protection Authority 2025).

Telemedicine remains relevant, but mainly as a confirming illustration rather than as a separate doctrinal centre. Remote monitoring, teleconsultation, and data flows generated outside traditional clinical premises show that digital healthcare is not confined to the elec-

tronic record. Yet their legal significance in the present argument lies precisely in the same point: the right to health is increasingly mediated through interoperable infrastructures, cybersecurity guarantees, differentiated access regimes, and institutional accountability for data environments rather than through one-off acts of consent alone (Conferenza Stato-Regioni 2020; Guaglianone et al. 2022; Gazzarata et al. 2024). What makes Italy analytically important is therefore not merely that it has digital-health reforms, but that it shows with unusual clarity how constitutional health protection is being reorganised through data governance (Murgia et al. 2025).

4. Secondary Use Beyond Consent: GDPR, Italian Law, and the EHDS

Secondary use is not inherently unlawful. The legal difficulty lies in identifying the conditions under which health data may be reused beyond immediate care, especially where consent is not relied upon or cannot realistically function as an effective individual control mechanism. Once health data cease to function only as instruments of immediate care and become resources for research, policymaking, public-health preparedness, regulation, and innovation, the traditional image of consent as the primary expression of self-determination becomes unstable (Becker et al. 2022; Italy 2003). Yet that instability should not be exaggerated into a simple narrative of consent's disappearance. The core doctrinal difficulties concern the choice of legal basis under Article 6 GDPR, the conditions of Article 9 for special-category data, compatibility of purposes, research and public-interest derogations, transparency, data minimisation, Article 89 safeguards, data-subject rights, access governance, function creep, and institutional accountability (European Parliament and Council 2016; Borg and Caruana 2024).

It is also necessary to distinguish the meanings of consent. Ethical or research consent concerns a person's willingness to participate in research and is central to research ethics, including the Declaration of Helsinki and, for health databases and biobanks, the Declaration of Taipei (World Medical Association 2024, 2016). GDPR consent is a specific legal basis for processing under Article 6, while explicit consent may operate as one of the Article 9 conditions for processing special categories of data. Consent to medical treatment concerns the lawfulness of the clinical act and the patient's self-determination in care. None of these concepts is identical to autonomy as a broader constitutional and ethical value. Keeping them distinct prevents both the overstatement and the premature dismissal of consent in digital healthcare (European Parliament and Council 2016; Borg and Caruana 2024; Hjort 2025).

Under the GDPR, data concerning health fall within special categories whose processing is prohibited unless one of the recognised conditions of Article 9(2) applies (European Parliament and Council 2016). The analysis of secondary use therefore cannot stop at the identification of a generic lawful basis. It must also consider whether the processing falls within a recognised derogation, whether the purposes are compatible, and whether the technical and organisational safeguards satisfy Article 89 GDPR (European Parliament and Council 2016; Becker et al. 2022; Rak 2024). This is why the move 'beyond consent' should be understood not as a deregulatory move, but as a shift toward a more demanding matrix of legal justification, institutional design, and controllable safeguards (European Parliament and Council 2016; Floridi and Taddeo 2016).

The Italian framework illustrates that logic with particular clarity. Articles 110 and 110-bis of Legislative Decree No. 196/2003 permit the processing of health data for medical, biomedical, and epidemiological research without consent in defined circumstances, especially where the research is grounded in law or Union law and where informing the data subjects proves impossible, entails disproportionate effort, or risks seriously prejudicing the research objective (Italy 2003). The intervention of the competent ethics committee

is not merely a formal procedural step. It introduces an external institutional actor into the balancing exercise and helps prevent the unilateral inflation of public-interest claims by controllers (Italy 2003; European Parliament and Council 2014; Schaefer et al. 2020). Where consent is not obtained, the protective function must therefore be performed by a combination of ethics review, documented necessity and proportionality, technical and organisational safeguards, and compliance with the safeguards prescribed by data-protection law and by the Italian DPA where applicable. The legal point is not that autonomy has become irrelevant, but that secondary use is tolerated only when institutional and procedural safeguards perform part of the protective work that consent cannot realistically perform in large-scale research environments (Borg and Caruana 2024; Hjort 2025).

The EHDS gives this transformation a much more explicit architecture. Regulation (EU) 2025/327 treats secondary use not as a marginal exception but as an organised and institutionalised component of digital-health governance (European Parliament and Council 2025). It does so through a structured system of Health Data Access Bodies, data permits or health data requests, restricted purposes, and secure processing environments rather than through fragmented ad hoc practices (Quinn et al. 2024; Rak 2024; Svingel et al. 2025). This matters because the legality of secondary use is increasingly mediated by the design of the governance environment: who may request access, for which purposes, under what conditions, through what technical environment, and subject to which audit and accountability constraints (European Parliament and Council 2025; Rak 2024).

That architecture also reveals why the opt-out debate cannot be reduced to symbolic invocations of control. The EHDS recognises a reversible right to opt out from secondary use, and Member States must provide mechanisms through which natural persons may exercise that right (European Parliament and Council 2025; Kruus 2025; Roussos 2025). At the same time, the Regulation allows Member States, under defined conditions, to provide exceptions, including for scientific research carried out for important reasons of public interest where the data cannot otherwise be obtained in a timely and effective manner. The real significance of the opt-out therefore depends on timing, intelligibility, public communication, and the institutional context in which the right is exercised. Formal agency without practical intelligibility is a weak proxy for self-determination in highly technical health-data ecosystems (Cervera de la Cruz et al. 2026). At the same time, the EHDS does not merely facilitate access; it also constructs prohibitions and use restrictions that are directly relevant to fairness, including limits on downstream uses that would be incompatible with the public-interest rationale of the system (European Parliament and Council 2025; Cervera de la Cruz and Shabani 2025).

The Data Governance Act adds a further layer to that landscape. Data altruism offers a channel for voluntary data sharing for purposes of general interest, but it should not be mistaken for an alternative constitutional foundation of secondary use (Yilmaz 2025; El Asry et al. 2025; European Parliament and Council 2022). Its significance is auxiliary and institutional: it shows that even voluntary sharing in the European data strategy is no longer imagined as a purely bilateral relation between data subject and controller, but as a mediated practice embedded within recognised organisational forms, governance duties, and supervision mechanisms (European Parliament and Council 2022).

These developments explain the growing importance of architecture-level safeguards. Pseudonymisation remains valuable, but contemporary debates rightly emphasise that pseudonymisation alone is not a complete answer (Rak 2024; Italy 2003). It reduces identifiability risk, but it does not transform personal data into anonymous data where re-identification remains reasonably possible. Health datasets are often rich, longitudinal, linkable, and clinically distinctive; rare conditions, demographic combinations, and linkage with external datasets may increase re-identification risk. The more convincing legal re-

sponse therefore lies in layered structures that combine pseudonymisation with controlled access, differentiated visibility, secure processing environments, purpose restrictions, audit logs, reviewable permits, and institutional accountability. The recent European Data Protection Board Guidelines 1/2026 on scientific research are especially significant in this respect because they reinforce the need to distinguish legal basis, special-category conditions, transparency, safeguards, and allocation of responsibilities rather than collapsing research processing into a single formula (European Data Protection Board 2026). The same logic also clarifies the place of synthetic data: useful in some contexts, potentially risk-reducing, but never self-sufficient as a doctrinal shortcut around governance requirements (Bartholdy 2026; Bonomi and Vasileiadou 2024).

Secondary use therefore does not show that consent has become irrelevant. It shows, rather, that data-subject protection increasingly depends not only on prior authorisation but also on governance design. Whether that development is legitimate depends not on general invocations of public interest, but on the legal quality of the framework that complements or compensates for consent's reduced practical centrality: differentiated purposes, reviewable permits, technical containment, proportionality, democratic accountability, and a meaningful residual place for the individual within a data-driven system (Becker et al. 2022; Rak 2024; Council of Europe 1950).

5. AI-Mediated Care as a Test Case for Governance, Information, and Responsibility

AI-mediated care is examined here because it shows how health-data governance reaches the clinical encounter. Data governance does not end when access to data is authorised; it shapes the datasets, validation practices, deployment choices, monitoring duties, and accountability channels through which AI systems enter clinical workflows. AI-mediated care therefore tests whether governance-based legality can remain compatible with autonomy, equality, meaningful information, human oversight, and responsibility once digital infrastructures begin to influence diagnosis, triage, treatment selection, and workflow management (European Parliament and Council 2024a; Kaltenbrunner 2026). The first doctrinal step is to distinguish among different forms of medical AI. Clinical decision-support systems, triage and prioritisation tools, AI embedded in regulated medical devices, and workflow systems do not raise identical issues for informed consent, human oversight, or liability. Without that basic typology, legal analysis quickly becomes either rhetorical or overgeneralised (Kaltenbrunner 2026; Dantas and Nogaroli 2021; Šustek and Šolc 2025).

The regulatory framework also applies in stages. The AI Act applies progressively: some provisions, including those on prohibited practices, AI literacy, governance, and general-purpose AI, have already entered into application, while certain high-risk obligations remain subject to later application dates and transitional arrangements, including for AI embedded in regulated products (European Parliament and Council 2024b; European Commission 2026). Nationally, Law No. 132/2025 confirms both the supporting role of AI in healthcare and the need to preserve the human centre of medical decision-making. Article 7 provides that the person concerned has the right to be informed about the use of AI technologies in healthcare, preserves the role of the healthcare professional in medical decision-making, and prohibits discriminatory selection or conditioning of access to healthcare services. Article 10 links AI support to the broader digital-health architecture by inserting Article 12-bis into the FSE legal framework and providing for ministerial decrees on AI solutions that support the functions connected to the electronic health record (Italy 2025).

This makes it essential to distinguish consent to treatment from GDPR consent. Under Law No. 219/2017, informed consent concerns the lawfulness of the medical act and the

patient's self-determination in relation to care (Italy 2017b). It is not equivalent to consent as a data-processing legal basis, nor can either concept be collapsed into the broader moral vocabulary of autonomy (Hjort 2025). Where AI contributes to clinical reasoning, legally adequate information cannot stop at the generic statement that 'AI was used'. At a minimum, the patient should be informed, in terms appropriate to the context, of the function of the system, the extent to which it informs or influences the clinical assessment, the relevant limits of the tool, and the fact that the final clinical decision remains attributable to human professionals (Italy 2025; Hjort 2025; Chau et al. 2025).

The difficulty, of course, lies in opacity. Algorithmic opacity may be commercial, epistemic, or explanatory, and those dimensions matter differently for institutions, clinicians, and patients (Nogaroli and Faleiros Júnior 2024). The law should not demand total transparency where that is technically unrealistic or clinically unhelpful. But neither can it tolerate a situation in which the patient receives no clinically meaningful account of how algorithmic mediation enters the decisional pathway. In this respect, explainability is best understood not as an absolute ideal of full intelligibility, but as part of a broader framework of contestability, traceability, and proportionate disclosure (Mourby et al. 2021; Panigutti et al. 2023; Hassan et al. 2025).

The same is true of human oversight. European and Italian law insist that AI in healthcare must remain under human control, but the formula is empty unless translated into institutional and professional conditions that make control real (European Parliament and Council 2024b; Italy 2025). Oversight requires competence, documentation, situational awareness, and genuine powers to question, override, or suspend algorithmic outputs. Otherwise, the physician may remain nominally in charge while automation bias, workflow dependence, or deskilling erode the capacity to exercise independent clinical judgment (Kaltenbrunner 2026; Kumar et al. 2025; Goffin 2025). The problem is therefore not solved by repeating that the doctor remains the final decision-maker; it is solved only if the surrounding legal and organisational environment enables the doctor to act as such in substance rather than in name (Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri 2014; Savulescu et al. 2024).

Bias and non-discrimination expose the same structural point from another angle. If AI systems perform differently across patient groups because of skewed data collection, annotation bias, poor validation, or deployment failures, then equality is jeopardised not by abstract algorithmic risk but by identifiable institutional omissions (Italy 1948; Kumar et al. 2025; Zarnegar 2026). Fairness cannot therefore remain a merely ethical aspiration. It requires validation across relevant groups, post-deployment monitoring, documentation, and governance structures capable of detecting and correcting systematic degradation in performance (Kumar et al. 2025; Zarnegar 2026). The legal significance of anti-discrimination in healthcare AI lies precisely in converting general equality commitments into operational duties of design, procurement, deployment, and review (Italy 2025).

AI also places pressure on the doctor-patient relationship, but that problem should be expressed in legal rather than purely anthropological terms. The issue is not simply that a 'third epistemic actor' enters the clinical encounter. More concretely, the relationship of care becomes legally thinner if the physician is reduced to a passive translator of machine-generated outputs and if the patient cannot identify where judgment, explanation, and responsibility are located (Greco and Picozzi 2022; Triberti et al. 2020; Lorenzini et al. 2023; Grote and Berens 2020). Trust remains relevant, but as a legal-structural concern tied to intelligibility and accountability rather than as free-standing rhetoric (Fiske et al. 2019).

These relational pressures culminate in the allocation of responsibility when harm occurs. Italian malpractice law still centres on professional responsibility and on the institutional responsibility of healthcare organisations under Law No. 24/2017 and the Civil

Code (Italy 1942, 2017a). Yet AI-mediated harm may stem from design flaws, poor training data, deficient organisational integration, negligent overreliance by clinicians, insufficient supervision, or combinations thereof (Šustek and Šolc 2025; Cohen et al. 2024). The older binary between physician error and technical malfunction is therefore increasingly unstable. A more precise analysis must distinguish professional medical liability, institutional liability of healthcare organisations, and the liability of software developers, producers, or technology providers (Bertolini 2020; Comandé 2019; Martín-Casals 2023; González-García Viñuela 2024).

At the professional level, clinician responsibility is strongest where the system is auxiliary and the physician retains a meaningful capacity to understand, contest, and depart from the output. At the institutional level, healthcare organisations may bear responsibility for procurement choices, validation before deployment, workflow integration, training, monitoring, incident reporting, and the prevention of foreseeable automation bias. At the producer or provider level, responsibility may arise where harm is linked to defective design, inadequate safety information, unsafe updates, cybersecurity weaknesses, or failure to correct known performance degradation. The allocation of responsibility will therefore depend on whether the tool is merely supportive, highly influential, opaque, adaptive, embedded in a regulated medical device, or integrated into organisational workflow. Liability is part of governance-based legality because it preserves an intelligible distribution of responsibility when consent, transparency, and formal human oversight are not sufficient by themselves.

The post-2025 liability landscape confirms the need for that matrix. The proposed AI Liability Directive is no longer a pending legislative horizon, having been officially withdrawn in 2025 (European Commission 2022). By contrast, Directive (EU) 2024/2853 now expressly adapts product liability to the digital economy and includes software within the product-liability framework, including defects linked to software updates or the lack of necessary safety updates (European Parliament and Council 2024a; Koch 2024). That is a significant step, but not a complete solution. Medical AI may be adaptive, probabilistic, and deeply embedded in institutional workflows; causation and proof remain difficult, especially where harm emerges through the interaction between software design, organisational deployment, and clinical reliance (Cohen et al. 2024; Duffourc and Gerke 2023). The legal challenge is therefore broader than compensation alone: it is to preserve an intelligible distribution of responsibility in a clinical environment increasingly mediated by complex technological systems.

6. Conclusions

Digital healthcare can no longer be understood adequately through the language of isolated processing operations or through a simple opposition between innovation and privacy. What is emerging in Italy and across the European Union is a more general reorganisation of healthcare around interoperable infrastructures, controlled conditions of reuse, and algorithmically mediated forms of support. In that environment, health data are not only protected objects; they are also the medium through which healthcare is coordinated, researched, and governed.

The central doctrinal implication is that legality is moving beyond consent-centred protection toward governance-based safeguards. This transition is not inherently incompatible with the right to health, but it is defensible only if constitutional coordination, data-protection safeguards, democratic accountability, and clinically meaningful responsibility are specified with precision. In the Italian context, this means that the FSE, the EDS, the interventions of the Italian DPA, the rules on research processing, and the health-

specific provisions of Law No. 132/2025 must be read together rather than as disconnected regulatory fragments.

Artificial intelligence confirms rather than displaces that conclusion. It shows that neither informed consent, nor transparency, nor formal physician primacy can function as a single all-purpose safeguard. What matters is whether law can articulate a layered framework in which differentiated access, secure processing environments, meaningful patient information, effective powers of intervention, anti-discrimination safeguards, and updated responsibility rules operate together. The future of digital healthcare therefore lies not in abandoning consent, but in specifying when and how lawfully designed governance may compensate for the reduced practical centrality of consent without sacrificing autonomy, dignity, equality, and accountability.

Author Contributions: Conceptualization, T.S., P.B., G.D. and G.R.; methodology, T.S., P.B. and G.P.; writing—original draft preparation, T.S. and P.B.; writing—review and editing, T.S., P.B., G.D. and G.R.; resources, project administration, and supervision, G.P. and G.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: No substantive legal analysis, data, or conclusions were generated by AI tools. DeepL free version and ChatGPT 5.2 were used only for language editing, syntax, and grammar checks. All legal analysis, citations, and final wording were reviewed and approved by the authors, and any discrepancy was resolved by restoring or revising the authors' original intended meaning.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
DPA	Data Protection Authority
EDS	Ecosystem of Health Data (Italian: Ecosistema Dati Sanitari)
EHDS	European Health Data Space
EU	European Union
FSE	Fascicolo Sanitario Elettronico (Italian electronic health record infrastructure)
GDPR	General Data Protection Regulation

References

Bartholdy, Mathias. 2026. Positioning synthetic data under EU data protection law. *Computer Law & Security Review* 61: 106310. [CrossRef]

Becker, Regina, Davit Chokoshvili, Giovanni Comandé, Edward S. Dove, Alison Hall, Colin Mitchell, Fruzsina Molnár-Gábor, Pilar Nicolàs, Sini Tervo, Adrian Thorogood, and et al. 2022. Secondary use of personal health data: When is it "further processing" under the GDPR, and what are the implications for data controllers? *European Journal of Health Law* 30: 129–57. [CrossRef]

Bertolini, Andrea. 2020. *Artificial Intelligence and Civil Liability*. Study Requested by the JURI Committee, PE 621.926. Brussels: European Parliament.

Bologna, Silvio, Alessandro Bellavista, Pietro Paolo Corso, and Gianluca Zangara. 2016. Electronic health record in Italy and personal data protection. *European Journal of Health Law* 23: 265–77. [CrossRef] [PubMed]

Bonomi, Sara, and Georgia Vasileiadou. 2024. Preserving privacy in European health research: The case of synthetic data. *Journal of Data Protection & Privacy* 6: 295–306. [CrossRef]

Borg, Roxanne Meilak, and Mireille Martine Caruana. 2024. Alternative legal bases for processing health data for scientific research purposes. *Masaryk University Journal of Law and Technology* 18: 3–26. [CrossRef]

Cervera de la Cruz, Patricia, and Mahsa Shabani. 2025. Fair enough? Exploring the role of fairness in secondary uses of health data in the European Health Data Space. In *The European Health Data Space: Examining a New Era in Data Protection*. Edited by Santa Slokenberga, Katharina Ó. Cathaoir and Mahsa Shabani. London and New York: Routledge, pp. 136–61.

Cervera de la Cruz, Patricia, Teodora Lalova-Spinks, and Mahsa Shabani. 2026. The European Health Data Space: An opportunity to strengthen citizen rights and engage citizens in health data governance. *Frontiers in Medicine* 12: 1699941. [CrossRef] [PubMed]

Chau, Michelle, M. G. Rahman, and Tarun Debnath. 2025. From black box to clarity: Strategies for effective AI informed consent in healthcare. *Artificial Intelligence in Medicine* 167: 103169. [CrossRef] [PubMed]

Cohen, I. Glenn, Andrew Slottje, and Sara Gerke. 2024. Medical AI and tort liability. In *Artificial Intelligence in Medicine: From Ethical, Social, and Legal Perspectives*. Amsterdam: Elsevier, pp. 89–104.

Comandé, Giovanni. 2019. Multilayered (accountable) liability for artificial intelligence. In *Liability for Artificial Intelligence and the Internet of Things*. Edited by Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer. Baden-Baden: Nomos; Oxford: Hart, pp. 165–84.

Conferenza Stato-Regioni. 2020. *Indicazioni nazionali per l'erogazione di prestazioni in telemedicina*; Bolzano: Le Regioni e le Provincie Autonome di Trento e di Bolzano.

Constitutional Court of Italy. 2002. *Judgment No. 282/2002*; Rome: Constitutional Court of Italy.

Council of Europe. 1950. *European Convention on Human Rights*. Strasbourg: Council of Europe.

Dantas, Eduardo, and Rafaella Nogaroli. 2021. The rise of robotics and artificial intelligence in healthcare: New challenges for the doctrine of informed consent. *Medicine and Law* 40: 15–62.

Duffourc, Mindy Nunez, and Sara Gerke. 2023. The proposed EU Directives for AI liability leave worrying gaps likely to impact medical AI. *npj Digital Medicine* 6: 77. [CrossRef] [PubMed]

El Asry, Eila, Juli Mansnérus, and Sandra Liede. 2025. Striking the balance: Genomic data, consent and altruism in the European Health Data Space. In *The European Health Data Space: Examining a New Era in Data Protection*. Edited by Santa Slokenberga, Katharina Ó. Cathaoir and Mahsa Shabani. London and New York: Routledge, pp. 110–35.

European Commission. 2022. *Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), COM(2022) 496 Final, Later Withdrawn on 6 October 2025*. Brussels: European Commission.

European Commission. 2026. *AI Act. Application Timeline. Shaping Europe's Digital Future*. Brussels: European Commission.

European Court of Human Rights. 2014. *L.H. v. Latvia, No. 52019/07, Judgment of 29 April 2014*. Strasbourg: European Court of Human Rights.

European Data Protection Board. 2026. *Guidelines 1/2026 on Processing of Personal Data for Scientific Research Purposes, Version Submitted to Public Consultation; Feedback Period 16 April–25 June 2026*. Brussels: European Data Protection Board.

European Parliament and Council. 2014. *Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on Clinical Trials on Medicinal Products for Human Use*. Brussels: European Parliament and Council.

European Parliament and Council. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. Brussels: European Parliament and Council.

European Parliament and Council. 2022. *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance (Data Governance Act)*. Brussels: European Parliament and Council.

European Parliament and Council. 2024a. *Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products*. Brussels: European Parliament and Council.

European Parliament and Council. 2024b. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Brussels: European Parliament and Council.

European Parliament and Council. 2025. *Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space*. Brussels: European Parliament and Council.

Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri. 2014. *Codice di Deontologia Medica, with Subsequent Updates*. Rome: Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri.

Fiske, Amelia, Peter Henningsen, and Alena Buyx. 2019. Your robot therapist will see you now: Ethical implications of embodied artificial intelligence in psychiatry, psychology, and psychotherapy. *Journal of Medical Internet Research* 21: e13216. [CrossRef] [PubMed]

Floridi, Luciano, and Mariarosaria Taddeo. 2016. What is data ethics? *Philosophical Transactions of the Royal Society A* 374: 20160360. [CrossRef]

Gazzarata, Roberta, Joao Almeida, Lars Lindsköld, Giorgio Cangioli, Eugenio Gaeta, Giuseppe Fico, and Catherine E. Chronaki. 2024. HL7 Fast Healthcare Interoperability Resources (HL7 FHIR) in digital healthcare ecosystems for chronic disease management: Scoping review. *International Journal of Medical Informatics* 189: 105507. [CrossRef] [PubMed]

Goffin, Tom. 2025. Does AI in healthcare need an editor-in-chief? A leading example of true human oversight. *European Journal of Health Law* 32: 78–95. [CrossRef]

González-García Viñuela, Maria. 2024. Responsabilidad por daños de productos y servicios sanitarios equipados con sistemas de inteligencia artificial. *Bioderecho.es* 19: enero–julio.

Greco, Francesca, and Mario Picozzi. 2022. Understanding the impact of artificial intelligence on physician-patient relationship: A revisitation of conventional relationship models in the light of new technological frontiers. *Medicina Historica* 6: e2022028.

Grote, Thomas, and Philipp Berens. 2020. On the ethics of algorithmic decision-making in healthcare. *Journal of Medical Ethics* 46: 205–11. [PubMed]

Guaglianone, Maria Teresa, Giovanna Aracri, Maria Teresa Chiaravalloti, Elena Cardillo, Camillo Francesco Arena, Elisa Sorrentino, and Anna Federica Spagnuolo. 2022. Ensuring the long-term preservation of and access to the Italian federated electronic health record. *Applied Sciences* 12: 3304. [CrossRef]

Hassan, Reda, Nhien Nguyen, Stine Rasdal Finserås, Lars Adde, Inga Strümke, and Ragnhild Støen. 2025. Unlocking the black box: Enhancing human-AI collaboration in high-stakes healthcare scenarios through explainable AI. *Technological Forecasting and Social Change* 219: 124265. [CrossRef]

Hjort, Live Sunniva. 2025. Informed consent to AI-based decisions in healthcare: Must patients understand the AI's output? *Oslo Law Review* 11: 1–21. [CrossRef]

Italian Data Protection Authority (Garante per la protezione dei dati personali). 2023. *Parere sullo schema di decreto del Ministero della salute recante "Fascicolo sanitario elettronico 2.0"—8 June 2023 [doc. web n. 9900433]*. Rome: Italian Data Protection Authority.

Italian Data Protection Authority (Garante per la protezione dei dati personali). 2024a. *Parere sullo schema di decreto del Ministero della salute recante "Fascicolo sanitario elettronico 2.0" e disciplina transitoria correlata*. Rome: Italian Data Protection Authority.

Italian Data Protection Authority (Garante per la protezione dei dati personali). 2024b. *Parere sullo schema di decreto del Ministero della salute sull'Ecosistema Dati Sanitari (EDS)—26 September 2024 [doc. web n. 10062302]*. Rome: Italian Data Protection Authority.

Italian Data Protection Authority (Garante per la protezione dei dati personali). 2025. *Parere sullo schema di decreto di modifica del decreto interministeriale n. 334 del 31 dicembre 2024, recante "Ecosistema dati sanitari" (EDS)—27 March 2025 [doc. web n. 10131261]*. Rome: Italian Data Protection Authority.

Italy. 1942. *Civil Code of Italy, Articles 1218, 1228, and 2043*. Rome: State of Italy.

Italy. 1948. *Constitution of the Italian Republic*. Rome: State of Italy.

Italy. 2001. *Constitutional Law 18 October 2001, No. 3. Amendments to Title V of Part II of the Constitution*. Rome: State of Italy.

Italy. 2003. *Legislative Decree 30 June 2003, No. 196. Personal Data Protection Code, as Subsequently Amended*. Rome: State of Italy.

Italy. 2012a. *Decree-Law 18 October 2012, No. 179. Further Urgent Measures for the Growth of the Country*. Rome: State of Italy.

Italy. 2012b. *Law 17 December 2012, No. 221. Conversion into Law, with Amendments, of Decree-Law No. 179/2012*. Rome: Gazzetta Ufficiale della Repubblica Italiana.

Italy. 2017a. *Law 8 March 2017, No. 24. Provisions on Patient Safety and Professional Liability of Healthcare Professionals*. Rome: State of Italy.

Italy. 2017b. *Law 22 December 2017, No. 219. Rules on Informed Consent and Advance Treatment Directives*. Rome: State of Italy.

Italy. 2023. *Decree of the Ministry of Health 7 September 2023. Fascicolo Sanitario Elettronico 2.0*. Rome: State of Italy.

Italy. 2024a. *Interministerial Decree 31 December 2024, No. 334. Ecosistema Dati Sanitari*. Rome: State of Italy.

Italy. 2024b. *Law 29 April 2024, No. 56. Conversion into Law, with Amendments, of Decree-Law 2 March 2024, No. 19, Especially Article 44*. Rome: State of Italy.

Italy. 2025. *Law 23 September 2025, No. 132. Disposizioni e deleghe al Governo in materia di intelligenza artificiale*. Rome: State of Italy.

Kaltenbrunner, Saskia. 2026. Human in control: Shared decision-making with clinical decision-support systems under the Artificial Intelligence Act. *Computer Law & Security Review* 61: 106281. [CrossRef]

Koch, Bernard A. 2024. Product liability on the way to the digital age. *Journal of European Tort Law* 15: 109–25. [CrossRef]

Kruus, Maret. 2025. Opting out of scientific research with health data: The limits of the EHDS and the GDPR. *European Journal of Health Law* 32: 165–89. [CrossRef] [PubMed]

Kumar, Rahul, Kyle Sporn, Ethan Waisberg, Joshua Ong, Phani Paladugu, Amar S Vadhera, Dylan Amiri, Alex Ngo, Ram Jagadeesan, Alireza Tavakkoli, and et al. 2025. Navigating healthcare AI governance: The comprehensive algorithmic oversight and stewardship framework for risk and equity. *Health Care Analysis*, *advance online publication*. [CrossRef] [PubMed]

Lorenzini, Georgia, Laura Arbelaez Ossa, David Shaw, and Bernice Elger. 2023. Artificial intelligence and the doctor-patient relationship: Expanding the paradigm of shared decision making. *Bioethics* 37: 931–40. [CrossRef]

Martín-Casals, Miquel. 2023. Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret* 3: 55–100.

Mourby, Miranda, Katharina Ó Cathaoir, and Catherine Bjerre Collin. 2021. Transparency of machine-learning in healthcare: The GDPR and European health law. *Computer Law & Security Review* 43: 105611. [CrossRef]

Murgia, Ylenia, Roberta Gazzarata, Mario Ciampi, Mario Sicuranza, Franco Cirillo, Christian Esposito, Norbert Maggi, Gabriella Balestra, Lucia Sacchi, Mauro Giacomini, and et al. 2025. The challenges of national health data ecosystems in feeding the European Health Data Space: The Italian example. *Frontiers in Medicine* 12: 1644719. [CrossRef] [PubMed]

Nittari, Giulio, Ravjyot Khuman, Simone Baldoni, Graziano Pallotta, Gopi Battineni, Ascanio Sirignano, Francesco Amenta, and Giovanna Ricci. 2020. Telemedicine practice: Review of the current ethical and legal challenges. *Telemedicine and e-Health* 26: 1427–37. [CrossRef] [PubMed]

Nogaroli, Rafaella, and José Luiz de Moura Faleiros Júnior. 2024. Ethical challenges of artificial intelligence in medicine and the triple semantic dimensions of algorithmic opacity with its repercussions to patient consent and medical liability. In *Multidisciplinary Perspectives on Artificial Intelligence and the Law*. Edited by Helena de Sousa Antunes, Pedro Miguel Freitas, Ana Lúcia Oliveira, Catarina Martins Pereira, Eduardo Vaz de Sequeira and Luís Barreto Xavier. Cham: Springer, pp. 229–48.

Panigutti, Cecilia, Ronan Hamon, Isabelle Hupont, David Fernandez Llorca, Delia Fano Yela, Henrik Junklewitz, Salvatore Scalzo, Gabriele Mazzini, Ignacio Sanchez, Josep Soler Garrido, and et al. 2023. The role of explainable AI in the context of the AI Act. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. New York: ACM, pp. 1139–50.

Presidenza del Consiglio dei Ministri. 2021. *Piano Nazionale di Ripresa e Resilienza, Missione 6 Salute*. Rome: Presidenza del Consiglio dei Ministri.

Quinn, Paul, Erika Ellyne, and Cong Yao. 2024. Will the GDPR restrain health data access bodies under the European Health Data Space (EHDS)? *Computer Law & Security Review* 54: 105993. [CrossRef]

Rak, Richard. 2024. Anonymisation, pseudonymisation and secure processing environments relating to the secondary use of electronic health data in the European Health Data Space (EHDS). *European Journal of Risk Regulation* 15: 928–38. [CrossRef]

Roussos, Antonis. 2025. The opt-out mechanism from secondary use in the European Health Data Space (EHDS) Regulation: Catalyst or barrier to patient engagement? *European Health and Pharmaceutical Law Review* 9: 158–70.

Savulescu, Julian, Alberto Giubilini, Rachel Vandersluis, and Abhishek Mishra. 2024. Ethics of artificial intelligence in medicine. *Singapore Medical Journal* 65: 112–18. [CrossRef]

Schaefer, G. Owen, Graeme Laurie, Sumytra Menon, and Teck Chuan Voo. 2020. Clarifying how to deploy the public interest criterion in consent waivers for health data and tissue research. *BMC Medical Ethics* 21: 23. [CrossRef] [PubMed]

Schwab, Klaus. 2016. *The Fourth Industrial Revolution*. New York: Crown Business.

Slokenberga, Santa, Katharina Ó Cathaoir, and Mahsa Shabani. 2025. Introduction: Transformation of electronic health data governance through the EHDS. In *The European Health Data Space: Examining a New Era in Data Protection*. Edited by Santa Slokenberga, Katharina Ó Cathaoir and Mahsa Shabani. London and New York: Routledge, pp. 3–21.

Svingel, Lise S., Caroline E. Jensen, Gitte F. Kjeldsen, Christian Fynbo Christiansen, Persephone Doupi, Nienke M. Schutte, and Damir Ivanković. 2025. Shaping the future EHDS: Recommendations for implementation of health data access bodies in the HealthData@EU infrastructure for secondary use of electronic health data. *European Journal of Public Health* 35: iii32–iii38. [CrossRef] [PubMed]

Šustek, Petr, and Martin Šolc. 2025. Civil liability for artificial intelligence in medicine: Is there a need for a new paradigm? *Lawyer Quarterly* 15: 40–58.

Topol, Eric. J. 2019. High-performance medicine: The convergence of human and artificial intelligence. *Nature Medicine* 25: 44–56. [CrossRef] [PubMed]

Triberti, Stefano, Ilaria Durosini, and Gabriella Pravettoni. 2020. A "Third Wheel" Effect in Health Decision Making Involving Artificial Entities: A Psychological Perspective. *Frontiers in Public Health* 8: 117. [CrossRef] [PubMed]

World Health Organization. 2021. *Ethics and Governance of Artificial Intelligence for Health*. Geneva: WHO.

World Medical Association. 2016. *WMA Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks, Adopted by the 53rd WMA General Assembly, Washington, DC, October 2002, and Revised by the 67th WMA General Assembly, Taipei, October 2016*. Ferney-Voltaire: World Medical Association.

World Medical Association. 2024. *WMA Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Participants, Adopted by the 18th WMA General Assembly, Helsinki, June 1964, and Revised by the 75th WMA General Assembly, Helsinki, October 2024*. Ferney-Voltaire: World Medical Association.

Yilmaz, Sabire Sanem. 2025. A legal perspective about "data altruism organization" and intermediaries service providers in European Health Data Space: Is a new hero for data subject? *Studies in Health Technology and Informatics* 326: 83–87.

Zarnegar, Armita. 2026. Addressing bias and ensuring fairness in AI systems for healthcare. In *HIKM '25: Proceedings of the 2025 18th Health Informatics Knowledge Management Conference, Article No. 1, 1–5*. New York: Association for Computing Machinery.