

RESEARCH

Open Access



Cyberspatial privacy in the digital age: a proxemics-based framework with a healthcare application

Orhan Onder^{1,2*} and Ebubekir M. Deniz³

Abstract

Background The rapid digitalization of healthcare—from telemedicine and Artificial Intelligence (AI)-driven diagnostics to wearable biosensors—has profoundly disrupted traditional norms of patient confidentiality. Classical privacy theories, anchored in physical co-presence and individual control, struggle to address the ethical challenges posed by opaque, persistent, and infrastructural data exposures in digital clinical environments.

Methods This study employs a theoretical-conceptual methodology to develop a multidimensional privacy framework responsive to the spatial and technological complexities of the digital clinic. Drawing from Edward T. Hall's proxemics theory and the concept of cyberspace, we reinterpret interpersonal spatial zones (intimate, personal, social, public) in cyberspace. We introduce "cyberspatial privacy" as a transversal dimension that modulates privacy expectations across physical and digital layers. A hypothetical case—"Patient X," a woman undergoing hybrid care—is used to demonstrate the framework's practical utility in ethical analysis.

Results The proposed framework reconceptualizes privacy as a dynamic continuum structured by both spatial proximity and digital mediation. By mapping risks across four proxemic zones and overlaying a cyberspatial dimension, the model reveals how privacy breaches differ not only in kind but in normative weight. For instance, biometric data collected by wearables (intimate zone) carries higher ethical risk than metadata exposed via public interfaces. The case of Patient X illustrates how classical theories fail to capture this gradient, while the new model enables zone-sensitive assessments of vulnerability, exposure, and trust.

Conclusions This framework advances the ethical understanding of privacy in digitally mediated healthcare by offering a granular, relational, and context-aware approach. It supports clinicians, designers, and policymakers in tailoring privacy safeguards to the spatial and digital contours of care. By reframing privacy as a condition of relational co-presence rather than isolated consent, this model promotes ethically robust design and governance in the era of cyber-augmented medicine.

Keywords Confidentiality, Privacy, Ethics, medical, Telemedicine, Digital health, Information systems, Health information management, Wearable electronic devices, Health policy, Medical informatics

*Correspondence:

Orhan Onder
orhan.under@marmara.edu.tr

¹Department of History of Medicine and Ethics, Marmara University, School of Medicine, Istanbul, Türkiye

²Department of Philosophy, Chair of Philosophy of Media and Technology, Vienna University, Vienna, Austria

³Istanbul Medeniyet University Philosophy Department, Istanbul, Türkiye



© The Author(s) 2025. **Open Access** This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

Background

Problematising privacy in contemporary healthcare

The digital transformation of healthcare has generated unprecedented ethical challenges for the protection of patient confidentiality. From electronic health records (EHRs) and AI-powered diagnostics to wearable monitoring devices and telemedicine platforms, healthcare is increasingly entangled with information and communication technologies (ICTs) that continuously collect, process, and transmit personal data [1, 2]. As medical practice shifts into hybrid clinical-digital environments, longstanding privacy expectations rooted in physical co-presence and direct interaction are being destabilized. The resulting ethical landscape exposes fundamental inadequacies in the conceptual tools historically used to safeguard privacy.

Conventional privacy frameworks—premised on notions of spatial seclusion, individual control, and informed consent—are increasingly outpaced by the structural features of digital systems. Data collection in digital health is often continuous, automated, and opaque, operating without explicit patient engagement or awareness [3, 4]. For example, biometric data gathered through smartwatches or implantable sensors may be transmitted to third-party servers, stored indefinitely, and processed algorithmically to generate behavioral or diagnostic inferences [5]. These processes occur within opaque data ecosystems that render boundaries between clinical, commercial, and governmental domains difficult to trace [6]. Such opacity is exacerbated when AI systems prioritize diagnostic efficiency over explainability, leaving patients unaware of how their data shapes clinical decisions [7]. In such contexts, breaches of confidentiality may no longer involve a singular act of unauthorized access, but rather a systemic erosion of informational boundaries.

Moreover, the ethical challenges are compounded by the temporal and spatial persistence of digital traces. Unlike verbal disclosures in the clinic, which are ephemeral and context-bound, digital interactions leave durable records that can be stored, replicated, and repurposed. As data circulates across interoperable platforms and interfaces, the ability to control its visibility becomes practically impossible, undermining core assumptions of both legal and philosophical accounts of privacy [8, 9]. These concerns are not hypothetical. Studies have documented privacy breaches resulting from data-sharing agreements, insecure telemedicine platforms, and algorithmic profiling of patients based on social media behavior or wearable devices [10, 11].

In clinical settings, the implications are especially profound. The confidentiality of the patient–physician relationship is traditionally anchored in spatial arrangements (e.g., the examination room), institutional protocols, and

norms of professional discretion. But when diagnostic tools, consultations, and monitoring devices operate within digital infrastructures, the very geometry of confidentiality is reconfigured. A patient may disclose sensitive information in a private consultation, yet the data may be captured by a telemedicine interface, processed by cloud-based analytics, and accessed by third-party vendors for secondary purposes [12, 13]. Here, confidentiality is no longer simply a matter of keeping a secret—it becomes a problem of structural exposure and distributed accountability.

This shift demands a reconceptualization of privacy in healthcare that can address:

- the opacity and scalability of digital data flows [14],
- the erosion of contextual boundaries [9],
- the invisibility of actors involved in data processing [15],
- and the new asymmetries of access and control [16].

Thus far, privacy theories have struggled to integrate these concerns in a unified ethical framework. Classical accounts emphasize individual autonomy [17], boundary regulation [18], or contextual appropriateness [9]. While each offers valuable insights, they are largely developed with assumptions rooted in face-to-face, spatially bounded, and agent-centric interactions. In hybrid clinical environments—where human actors, digital interfaces, and algorithmic systems are entangled—these conditions no longer hold. There is a growing need for a model that captures the relational, spatial, and technological reconfigurations that now shape privacy experience.

Limits of classical privacy theories

Foundational theories of privacy—such as those developed by Westin [17], Altman [18], Petronio [19], and Nissenbaum (2010)—have long shaped our understanding of informational boundaries and interpersonal disclosure. These models emphasize various dimensions of privacy: Westin focuses on individual control over personal information; Altman presents privacy as a dynamic process of boundary regulation; Petronio introduces the notion of co-ownership and rule-based management of private information; and Nissenbaum foregrounds contextual appropriateness in the flow of information. While these frameworks remain influential, many of them were originally developed in the context of face-to-face interaction, clearly demarcated physical settings, and agent-driven decisions. As such, they require reexamination or expansion to fully account for the complexities of privacy in digitally mediated and hybrid clinical environments.

Such assumptions become inadequate in digital health environments characterized by non-spatial, automated, and persistent data exposures. In particular, these

models struggle to account for the algorithmic inference, opaque surveillance, and structural asymmetries that define contemporary information ecosystems [3, 6, 20]. For instance, consent-based models presuppose that individuals are aware of and can meaningfully control the circulation of their data—an increasingly untenable assumption in systems governed by real-time data analytics and interoperable platforms [8, 21]. As Bak et al. [7] aptly note, “when it comes to AI, we sometimes seem to forget that data access is the most important prerequisite for any AI innovation,” underscoring the disconnect between privacy protections and the operational demands of data-intensive systems. Similarly, Nissenbaum’s theory of contextual integrity, although attuned to social norms, relies on relatively stable contexts and actor identifiability—both of which are destabilized in digitally networked systems where context collapses and data is repurposed across domains [22].

More fundamentally, classical privacy theories lack a spatially and relationally sensitive vocabulary capable of describing how proximity, visibility, and vulnerability are reshaped in cyberspace. They offer few conceptual resources for distinguishing between different *degrees* of privacy exposure within digital interactions. As a result, they fall short of addressing privacy harms that arise not only from unauthorized access, but from the shifting topology of digital presence itself—where data flows, algorithmic associations, and mediated disclosures reconfigure the boundaries between intimate, personal, social, and public spheres [16, 23].

This conceptual limitation is particularly problematic in clinical settings, where patient privacy is historically linked to spatial arrangements and direct communicative acts. When health data is collected via wearable sensors, exchanged on telemedicine platforms, or stored in cloud-based infrastructures, the spatial logic that once supported confidentiality becomes inadequate. To safeguard patient confidentiality in the digital era, an ideal framework of privacy must move beyond traditional spatial assumptions and address the ethical complexity introduced by digitally mediated clinical environments.

The need for a conceptual shift

The emergence of cyberspace—the socio-technical domain generated by the global integration of internet-based networks, digital infrastructures, and algorithmic systems—has profoundly altered the spatial, temporal, and relational conditions under which privacy is experienced and negotiated. Far from serving as a mere extension of physical environments, cyberspace constitutes a qualitatively distinct realm in which traditional boundaries between bodies, spaces, and information are persistently reconfigured [24, 25]. Within this domain, interactions occur not through physical co-presence but

via interfaces, data streams, and computational logics that render individuals visible, accessible, and interpretable across time and context [26, 27].

The implications of this shift are particularly significant in healthcare, where digital infrastructures mediate increasingly intimate aspects of human life. From telehealth consultations to wearable biometric devices and AI-driven diagnostics, patients’ bodies, emotions, and behaviors are now routinely encoded into digital signals and subjected to automated processing [12, 28]. These forms of exposure are not merely informational but structurally embedded in the logic of continuous data collection and algorithmic monitoring, reshaping traditional expectations of bodily privacy and autonomy [29].

While existing theories of privacy offer valuable insights, they often lack the conceptual tools to fully capture how digital proximity operates in cyberspace. Unlike analog proxemic interactions, where spatial proximity directly corresponds to sensory co-presence and mutual awareness, digital mediation fundamentally transforms this correspondence: cyberspatial ‘proximity’ is constituted not by physical distance but by data exposure, interface architecture, and algorithmic visibility. Thus, while Hall’s zones remain conceptually relevant as gradations of relational intimacy, their digital instantiation operates through fundamentally different material substrates—rendering what was once ephemeral and spatially bounded into persistent, replicable, and infrastructurally diffuse traces. What is needed is a more expansive framework—one that reflects the gradual, relational, and zone-sensitive nature of privacy in digitally mediated environments. Such a framework would recognize that in cyberspace, exposure is not necessarily voluntary, nor always reducible to a single act of consent. Moreover, recent work on AI-mediated clinical practice shows that algorithmic opacity can shift trust and responsibility back onto clinicians, reinforcing that privacy and trust in digital medicine are structurally intertwined rather than merely informational [30]. Conceptually, this means that privacy emerges as a dynamic condition shaped by one’s ongoing relation to overlapping digital infrastructures, algorithms, and audiences—many of which remain invisible or unknowable to the individual [20, 31].

To construct such a model, we turn to Edward T. Hall’s proxemics theory [32, 33], which offers a structured typology of interpersonal spatial zones—intimate, personal, social, and public—each associated with distinct relational norms and communicative expectations. Though developed in analog settings, Hall’s framework provides a powerful conceptual tool for rethinking privacy as a matter of graduated relational distance, not absolute separation. We argue that these spatial zones can be productively extended into cyberspace, where digital interactions likewise differ in degree and

character—from encrypted private messaging to algorithmically visible social media activity.

In this context, we introduce the concept of cyberspatial privacy as a transversal dimension that intersects all four proxemic zones. Rather than conceptualizing digital privacy as a discrete or fifth category, we propose that digital mediation infiltrates and reshapes each zone of human interaction, altering the expectations and vulnerabilities traditionally associated with them. For example, a medical consultation conducted through a telemedicine platform may occupy the “intimate” zone in terms of its content but simultaneously be exposed to “public” risks through insecure servers or third-party data access.

The aim of this article is to develop a multidimensional privacy classification framework that reclassifies privacy expectations across physical and digital spaces in a manner that is both spatially grounded and technologically attuned. While concepts such as Floridi’s *infosphere* help situate these changes within a broader ontological narrative [34], our focus is on cyberspace as an operational domain in which healthcare interactions now routinely unfold. By integrating proxemic theory with a cyber-oriented analysis of digital mediation, this framework provides a scalable, zone-sensitive tool for understanding how privacy is structured, breached, and protected in the contemporary digital clinic.

This reconceptualization holds significant practical implications: it enables clinicians, designers, and policymakers to assess privacy not only by what data is disclosed, but by how, where, and in which relational context such disclosure occurs.

Methods

This study adopts a theoretical-conceptual methodology aimed at developing a novel framework for understanding privacy in the context of digitally mediated healthcare. Rather than relying on quantitative or qualitative empirical data, the approach centers on the reinterpretation and extension of existing theoretical resources to address normative and structural problems that have emerged with the rise of digitally mediated clinical practices. This method is grounded in traditions of conceptual analysis and critical theory, which are well-established in normative ethics, philosophy of technology, and information studies [35, 36].

Conceptual strategy

The goal of this study is to articulate a multidimensional, zone-sensitive classification of privacy that can address the limitations of existing public/private or control-based models in the age of pervasive digital mediation. To achieve this, we engaged in a multi-stage conceptual process involving the synthesis, reinterpretation, and transposition of existing frameworks:

- First, we conducted a critical review of dominant theories of privacy—particularly those by Westin [17], Altman [18], Petronio [19], and Nissenbaum [9]—to identify their common assumptions and structural limitations when applied to cyberspace and healthcare contexts.
- Second, we selected two complementary theoretical foundations as the basis for a reconceptualization of privacy: (1) Edward T. Hall’s proxemics theory, which offers a relational and spatial account of interpersonal zones (intimate, personal, social, public), and (2) The concept of cyberspace—understood as a socio-technical domain constituted by networks of digital infrastructures, where algorithmic systems dynamically reshape proximity, visibility, and interactions [9, 37, 38].
- Third, we adapted Hall’s proxemic model to cyberspace by reinterpreting the original spatial zones as gradations of digital relational proximity, shaped not by physical distance but by levels of informational exposure, algorithmic mediation, and access control.

This process resulted in a conceptual framework that introduces cyberspatial privacy as a transversal dimension that intersects all four proxemic zones. This innovation allows us to theorize privacy in contemporary healthcare as a multidimensional phenomenon structured by varying intensities of exposure across both spatial and digital layers.

Illustrative validation through case analysis

To evaluate the practical relevance and explanatory power of the proposed framework, we apply it to a hypothetical but realistically constructed case of “Patient X”—a woman receiving hybrid gynecological care involving in-person consultation, biometric monitoring through a wearable device, and a telemedicine follow-up session. This case, presented in the discussion section, serves as an illustrative application rather than empirical validation. It is used to demonstrate how the framework can be employed to map distinct privacy expectations and risks across spatial and digital domains.

In ethical theory and conceptual design, such use-case analysis is a recognized method of demonstrating theoretical adequacy, especially when addressing emerging technological phenomena that lack stable empirical generalizations [39, 40].

Justification of theoretical approach

The decision to use a conceptual methodology is grounded in the recognition that new ethical problems—especially those arising from structural and infrastructural transformations—often require the development of

new conceptual tools [41]. Digital health environments pose challenges that are not only empirical but ontological and normative, necessitating frameworks capable of addressing the changing conditions of human interaction, embodiment, and visibility.

This approach aligns with prior work in philosophy of technology and information ethics that emphasizes:

1. Anticipatory Analysis: The need to design frameworks that anticipate, rather than merely describe, ethical dilemmas [42, 43], particularly in contexts where empirical data is scarce or evolving [39].
2. Use-Case Validation: The methodological legitimacy of applying hypothetical but plausible cases to test theoretical robustness, especially for emerging technologies that disrupt traditional norms [40, 44]. As Swierstra [44] argues, "techno-moral vignettes" (e.g., our Patient X case) reveal how technologies reconfigure moral expectations, making them indispensable for conceptual ethics.

The resulting framework reframes privacy as a *dynamic negotiation of relational and informational boundaries* across proxemic zones. This shift mirrors broader critiques of static privacy theories in digital environments [9, 34] while offering a practical tool for clinical ethics consultation.

Results: the cyberspatial privacy framework

This section presents the core contribution of the study: a multidimensional privacy classification framework developed through the conceptual adaptation of Edward T. Hall's proxemics theory into the domain of digitally mediated healthcare. The proposed framework reinterprets privacy as a dynamic continuum of relational proximity and exposure, shaped simultaneously by spatial context and digital mediation.

Hall's proxemic theory, originally developed to describe patterns of interpersonal distance and communication [33, 45], defines four spatial zones: intimate, personal, social, and public. Each zone is associated with different levels of emotional closeness, disclosure expectations, and interactional norms. This study extends these spatial zones into cyberspace, proposing that digital environments introduce a new layer of mediation—here termed cyberspatial privacy—that intersects and reconfigures each proxemic zone.

The result is a circular, zone-based privacy model with a transversal cyberspatial dimension. This dimension acknowledges that contemporary privacy violations are not confined to specific digital settings but cut across the full range of human interaction—from private communication to public self-presentation. In this model,

privacy risk is not a function of proximity alone, but of how spatially-situated interactions are infiltrated and restructured by digital infrastructures, platforms, and algorithms.

From spatial to cyberspatial zones of privacy

At the heart of the model is a set of four concentric relational zones—intimate, personal, social, and public—originally defined in terms of physical distance but here reinterpreted through informational and algorithmic proximity. These are overlaid with a cyberspatial layer, representing the structural conditions that define exposure, access, and mediation in digital contexts. This model allows privacy concerns to be mapped not only by the type of interaction, but by the intensity and digital permeability of each zone.

We present below the defining features and digital vulnerabilities of each zone.

Intimate privacy

In physical contexts, intimate privacy involves interactions that require close bodily proximity and high emotional sensitivity—such as whispered conversations, personal disclosures within the home, or physical examinations in clinical settings [33]. These interactions are governed by strong expectations of seclusion, trust, and minimal external exposure.

In digital contexts, intimate cyberspatial privacy encompasses the storage and exchange of highly sensitive personal data, including medical records, biometric and genetic data, and private conversations conducted through encrypted messaging platforms. Breaches in this zone often involve unauthorized access to functional MRI data [46], non-consensual dissemination of private photos or videos [47], or interception of confidential medical communication [48]. Although such interactions may appear private, they are increasingly vulnerable to malware, metadata leakage, or third-party surveillance.

Personal privacy

Personal privacy pertains to semi-private social contexts involving trusted friends or colleagues—for example, workplace conversations, informal gatherings, or one-on-one discussions. These interactions involve moderate disclosure, selective access, and expectations of discretion [49, 50].

In cyberspace, personal privacy includes friend-restricted social media content, private chat groups, video calls, and behavioral data shared on supposedly secure platforms. Risks arise when platforms employ emotional profiling—for example, analyzing facial expressions or text to infer mental states and target users with ads [51]. Even when access is limited to a

known audience, users' behavioral data may be captured, inferred, or shared without their knowledge.

Social privacy

Social privacy governs interactions with acquaintances, colleagues, or community members in formal or semi-public spaces—such as team meetings, professional conferences, or local events. These contexts are structured by reputational norms and limited self-disclosure.

In cyberspatial terms, social privacy refers to participation in online communities, workplace collaboration tools (e.g., Zoom, Slack), and public-facing social media groups. Here, users are susceptible to group-based targeting, engagement tracking, or algorithmic profiling, even in contexts that feel socially bounded. What begins as an informal digital interaction—e.g., participating in a support forum—can become part of a larger data set used for advertising or political campaigning [27].

Public privacy

Public privacy refers to interactions in anonymous or large-scale settings, such as public speaking, protests, or interacting with strangers in open environments. While expectations of privacy are lowest here, individuals still seek to retain control over their identity and representation.

In cyberspace, this includes publicly visible profiles, open comments, and search-indexed posts. Even if such content is voluntarily disclosed, aggregation and recombination of data by third-party systems can lead to identity theft, doxxing, or unwanted surveillance [52]. Anonymity becomes increasingly difficult to maintain due to facial recognition, persistent identifiers, and algorithmic de-anonymization techniques.

Cyberspatial privacy as a transversal dimension

Unlike models that treat digital privacy as a separate or additive category, this framework conceptualizes cyberspatial privacy as a transversal force—a mediating layer that permeates and reshapes all four spatial zones. In the digital age, proximity is no longer defined solely by physical distance, but by data exposure, interface design, and algorithmic access. Interactions that once felt secure due to spatial containment are now subject to persistent, automated, and context-collapsing forms of mediation.

Consider the following cross-zone transformations:

- In the intimate cyberspatial zone, encrypted messaging mimics whispering—but remains vulnerable to metadata analysis or malware interception.
- In the personal cyberspatial zone, emotionally expressive posts shared within trusted networks are

subject to AI-driven sentiment analysis for targeted marketing.

- In the social cyberspatial zone, workplace calls via Zoom expose users to behavioral tracking, background visibility, and potential data logging.
- In the public cyberspatial zone, seemingly anonymous online participation is undermined by surveillance technologies that aggregate, infer, and reidentify.

Discussion: applying the framework in clinical contexts

Case introduction: patient X

To illustrate the practical implications of our theoretical framework, we begin by examining a realistic scenario:

Patient X, a 35-year-old woman in a high-pressure tech career, visits her gynaecologist for a routine checkup at a specialised women's health clinic. During the initial consultation, the doctor collects history, including a family history of pre-menopausal breast cancer, the patient's desire to start a family, and reports of occasional dizziness and heart palpitations that the patient attributes to work stress. Following the gynecological examination, and given the complex familial and symptomatic picture, the doctor not only recommends a 24-hour heart rhythm monitor but also proposes a comprehensive genetic screening panel. Patient X consents to both, signing a digital form with broad language permitting the use of her data for "anonymous research and development." A follow-up consultation is scheduled via a telemedicine application to discuss the results from the wearable device and the genetic test. Unbeknownst to Patient X, her journey creates a cascade of data exposures: her personal fitness tracker and period-tracking app sync and sell anonymized data to a health aggregator, which is later accessed by her company's wellness program; the telemedicine platform uses a third-party service to collect interaction metadata; and the cloud database of the clinical-grade wearable is later involved in a breach, creating a risk of her intimate health data being re-identified and exposed publicly.

This scenario demonstrates multiple dimensions of privacy concerns across intimate, personal, social, and public zones, as mediated through both physical and digital interactions. Using this case as a foundation, we critically assess classical theories of privacy and subsequently apply our cyberspatial privacy framework to illuminate its analytical and ethical advantages. While Patient X illustrates the framework's application, it is important to note that basing ethical analysis on a single case has

limitations. The particularities of this scenario may not fully represent the range of patient experiences in digital healthcare. However, we find it of critical importance to share this illustration as it demonstrates the framework's relevance in real-world contexts.

A critical reassessment of classical privacy theories

The case of *Patient X* reveals the limitations of classical privacy theories when confronted with the complexities of digitally mediated healthcare. As previously discussed, the foundational models developed by Westin [17], Altman [18], Petronio [19], and Nissenbaum [9] each foreground key dimensions of privacy—control, boundary negotiation, co-ownership, and contextual integrity, respectively. Yet these approaches share certain structural assumptions: they presume clear agent boundaries, spatially bounded interactions, and contextual stability. Such conditions are increasingly absent in cyber-augmented clinical environments.

For instance, Westin's notion of privacy as control over personal information becomes strained when data generated by wearable devices is continuously transmitted and processed without the patient's active intervention or ongoing awareness. In *Patient X*'s case, her consent to share data is framed in broad, ambiguous terms, showing how Westin's focus on control becomes inadequate in the age of continuous and opaque data flows. Altman's model of boundary regulation, while more dynamic, still presumes a physical-social setting in which individuals can modulate access based on proximity and cues. In contrast, cyberspace often precludes awareness of who is accessing one's data, when, and for what purpose—rendering traditional mechanisms of regulation insufficient. However, the constant synchronization of *Patient X*'s fitness and period-tracking apps with health aggregators complicates her ability to regulate her boundaries, as digital mediation erodes traditional concepts of boundary control.

Petronio's theory of communication privacy management highlights co-ownership and rules of disclosure, yet digital environments radically destabilize the notion of discrete co-owners. Patient data may be shared across institutional boundaries, repurposed for research or algorithmic training, or accessed by technical personnel with no relational connection to the patient. Finally, Nissenbaum's contextual integrity framework relies on stable informational norms within well-defined contexts. But in digitally mediated healthcare, context collapse—in which data circulates across professional, commercial, and even public domains—undermines the very integrity of context [22]. For instance, *Patient X*'s data, once confined to the medical context, is shared across multiple sectors (workplace wellness programs, third-party services), illustrating how context collapses in digitally mediated

environments, as predicted by Nissenbaum's theory of contextual integrity.

What these theories lack is a mechanism to account for how cyberspatial mediation alters the geometry of privacy—not merely its ownership, but its shape, reach, and durability. The proxemics-based framework developed in this article offers a corrective by reclassifying privacy as a multidimensional structure shaped by both spatial proximity and digital permeability. It shifts attention away from isolated data points or consent events, and toward zones of relational expectation and technological vulnerability. This approach allows us to better diagnose the ethical risks that arise when spatial and digital dimensions intersect, as they do in the care of *Patient X*.

Case study: applying the framework to patient X

The case of *Patient X*, a 35-year-old woman undergoing routine gynecological care, serves as a concrete demonstration of how privacy vulnerabilities can be analyzed across the spatial–cyberspatial zones defined in our framework. Her experience spans multiple dimensions of intimacy, from physical examination to wearable data monitoring, and from genetic testing consent to data exposure via telemedicine and workplace wellness programs. These interactions reveal how digital mediation transforms traditional expectations of confidentiality and exposes new ethical tensions, especially in hybrid clinical environments.

Intimate zone: bodily proximity and biometric surveillance

The physical gynecological examination exemplifies spatial intimate privacy, where the proximity of bodies and the sensitivity of disclosed information demand strong protections of trust, dignity, and confidentiality. Examination rooms are designed to shield patients from public exposure, limiting both physical access and auditory disclosure. Yet, intimate privacy no longer resides solely within the walls of the clinic. In the case of *Patient X*, the gynecological examination is only one aspect of the intimate privacy experience. The data generated from her wearable device and genetic tests adds a layer of surveillance, which shifts the ethical burden from physical protection to safeguarding digital interfaces and encrypted data exchanges.

The recommendation of a 24-hour heart rhythm monitor introduces significant cyberspatial intimate privacy concerns. The wearable device collects continuous biometric data—heart rate, variability, sleep patterns, and potentially emotional stress indicators—transforming the patient's body into a data-producing interface [1, 53]. This data, if inadequately encrypted or stored on third-party servers without robust access controls, can be vulnerable to interception, unauthorized use, or secondary analysis [11]. While such devices are often marketed for patient

empowerment, they simultaneously expose patients to persistent and algorithmically mediated surveillance [29]. Furthermore, as Patient X's health data synchronizes with a third-party platform, the very essence of her intimate privacy is altered. Data that she considers for personal health management becomes part of a broader, commercially influenced ecosystem, exposing her to the risk of data re-identification and unauthorized secondary uses, such as health profiling or predictive analytics.

Genetic testing represents an increasingly common layer of intimate data collection in healthcare. Genetic information, which implicates not only the individual but their biological relatives, intensifies the ethical stakes of data protection [54, 55]. Regulatory measures such as the General Data Protection Regulation (GDPR) and HIPAA provide baseline protections. These frameworks often fail to address secondary uses of genetic data—such as algorithmic training or insurance risk assessments—that occur beyond the clinical context [56]. Emerging concerns about data portability, reidentification, and predictive inference necessitate more granular safeguards—particularly around consent procedures, encryption at rest and in transit, and long-term storage governance [2, 57, 58]. For Patient X, consent for genetic testing—embedded within the digital forms of broad research consent—becomes a significant privacy concern. Her genetic data, while ostensibly anonymous, may contribute to predictive models or research initiatives with far-reaching implications, making her sensitive biological information vulnerable to future reidentification and non-consensual commercial use.

Personal zone: telemedicine and the domestic–digital interface

Spatial personal privacy is foregrounded in the semi-private clinic spaces—waiting rooms and consultation areas—where Patient X may encounter others, overhear conversations, or inadvertently disclose information. These spaces are governed by weaker but still significant privacy expectations, where environmental design (e.g., physical barriers, noise dampening) and procedural controls (e.g., limiting unnecessary personnel) are vital to upholding discretion.

Digitally, this zone extends to telemedicine consultations, where private discussions occur within the ostensibly secure space of the patient's home. Yet home environments are not inherently private in the digital sense; telemedicine platforms may capture metadata, store logs, or default to open settings that compromise confidentiality [59]. Without end-to-end encryption, granular privacy settings, and strict access controls, the boundary between personal and institutional domains is blurred [60].

Moreover, the platform infrastructure may include data tracking, behavioral profiling, or integration with third-party services, which patients may be unaware of or unable to control as in the case of Patient X. Ethical telemedicine design must therefore integrate transparency, auditability, and minimal data collection as core principles—not merely as compliance features but as structural safeguards for cyberspatial personal privacy [61].

Social zone: clinics as semi-public environments and networked communities

Patient X's spatial social privacy may be compromised in seemingly benign contexts such as clinic waiting rooms, where her presence at a women's health clinic could imply sensitive health issues. Even without verbal disclosure, the visibility of place can signal private information to observers [9].

Cyberspatial social privacy is similarly at risk when patients' information becomes visible across online health forums, data repositories, or institutional communications. If her anonymized data from the wearable device is shared for research without meaningful consent—or if providers discuss her case in digital settings where she can be reidentified—this constitutes a breach of the social zone [62]. Compounding the risk is the potential repurposing of data for commercial use, such as in targeted clinical advertising that draws on patient narratives. Without explicit opt-in, these practices risk transforming the therapeutic relationship into a commodified one, eroding trust and autonomy [6, 16].

The sharing of case studies online or at conferences, even when anonymized, poses a further challenge. As demonstrated in prior research, patients can often be reidentified through cross-referencing small details [63]. Thus, even ethically motivated dissemination of clinical insights must be evaluated through the lens of cyberspatial social zone vulnerabilities.

Public zone: data breaches and the uninvited spectator

Although Patient X does not voluntarily enter public disclosure, her privacy may be compromised through institutional data breaches, misconfigured databases, or search engine visibility. If her name is visible on a public appointment list, or if the clinic shares anonymized data sets without adequate deidentification protocols, cyberspatial public privacy is at risk. In recent years, numerous breaches of healthcare systems have led to mass exposure of sensitive patient records—underscoring that public exposure is no longer a matter of intent, but of infrastructure and governance [64].

Moreover, with the expansion of predictive analytics and AI in clinical decision-making, data collected in

clinical settings may feed into opaque systems whose outputs are deployed in other domains—insurance eligibility, workplace assessments, or credit scoring—without the patient's knowledge or recourse [21, 65]. These risks exemplify how cyberspatial public exposure extends beyond the clinical domain, reinforcing the importance of structural protections that are zone-specific and anticipatory.

Through this case, we demonstrate that privacy in digital healthcare is not monolithic, and that breaches are not equal in ethical intensity or effect. Our multidimensional framework allows for a differentiated analysis that reflects the emotional, spatial, and infrastructural context of each privacy zone. By mapping vulnerabilities in both spatial and cyberspatial terms, this model offers practical insights for privacy-enhancing design, policy-making, and professional conduct.

Enhancing ethical sensitivity in healthcare design and practice

By introducing *cyberspatial privacy* as a transversal dimension that permeates all zones of human and technological interaction, our framework advances a more granular, situated, and ethically responsive model of privacy in healthcare. This conceptual structure enables the following key contributions:

Differentiated ethical risk assessment

Not all privacy violations carry equivalent normative weight. A breach involving intimate biometric data—such as continuous heart rhythm patterns or genomic information—invokes fundamentally different ethical imperatives than the inadvertent exposure of public-facing metadata [2, 66]. Our zonal model facilitates context-sensitive triaging of privacy risks, allowing clinicians, technologists, and policymakers to calibrate their responses based on the type, proximity, and reusability of the exposed data.

Zone-calibrated system design

Current healthcare information systems often rely on uniform security protocols that do not reflect the ethical variability of the data they handle [67]. Our framework supports a more responsive and layered approach to system architecture. For instance, technologies processing intimate or personal health data should implement stricter encryption, minimize data persistence and logging by default, and include granular access control with real-time auditability [68]. In contrast, systems engaged at the public or social zones should emphasize user awareness, informed consent, and visibility of downstream data flows, in line with principles of digital transparency [61].

Reframing consent and control

Classical privacy frameworks frequently rely on one-time, checkbox-style consent mechanisms that assume an individualistic, liberal conception of autonomy—an approach increasingly critiqued for its inadequacy in the context of big data [69]. However, in digital health environments characterized by persistent data collection and opaque algorithmic mediation, consent must be reconceptualized as continuous, situated, and structurally aware. Similarly, informational control should not be equated with mere possession or revocability of data but understood as the relational modulation of exposure and risk across shifting proximity zones [70]. This shift opens the way for new tools—such as context-sensitive privacy dashboards and zone-specific user interfaces—that support patients in dynamically managing their privacy.

Supporting clinical and regulatory reflexivity

Beyond system design, our model also serves as a pedagogical and regulatory instrument. For clinicians, it provides a language and structure to recognize privacy not only as a legal obligation but as an ethical space of relational responsibility [71]. For policymakers and standards bodies, the framework offers a normative infrastructure for crafting *zone-sensitive* privacy guidelines, moving beyond abstract principles toward operational criteria that match the degree and type of cyber-physical mediation involved in each healthcare process.

Democratization of healthcare

As healthcare becomes more digitally mediated, there is an increasing opportunity for democratizing care. Digital health tools, particularly AI-driven systems, enable patients to gain greater control over their health data and decisions, bridging gaps in healthcare equity, especially for marginalized communities. The democratization of healthcare is not only about increasing access to care but also about empowering patients with the autonomy to manage their health information. This perspective aligns with Hendl's observation that digital health technologies provide patients with a voice in their care, fostering inclusivity and transparency [72]. Within the context of privacy, our framework supports this shift by ensuring that privacy safeguards are not only technologically robust but also accessible to all patients, promoting patient autonomy in managing their data.

Global perspective and the GPOC initiative

Moreover, the global nature of healthcare in the age of digital mediation amplifies privacy challenges. Data privacy and protection issues transcend national borders, making it essential for digital health initiatives to prioritize international cooperation in privacy regulation, particularly with the rise of AI and telemedicine. A key

example of this trend is the Global Patient co-Owned Cloud (GPOC) initiative, which explores shared ownership of health data across borders. This initiative presents a model for healthcare data management that resonates with our proposed privacy framework, where patients retain control over their data while enabling cross-border collaboration. As highlighted in recent studies [73–75], GPOC exemplifies the future of data ownership, where privacy, control, and accessibility intersect across global healthcare systems.

Toward a new normative geometry of privacy

The clinical case of Patient X exemplifies the entanglement of bodily, informational, and infrastructural elements in contemporary healthcare. It reveals that legacy privacy theories, while foundational, remain insufficient to capture the complex configurations of exposure, mediation, and vulnerability instantiated in hybrid clinical environments. Accordingly, our framework calls for a *new normative geometry of privacy*—one that is attuned to spatial and digital dynamics, and capable of informing ethical evaluation, design foresight, and policy innovation.

This new geometry rests on the principle that privacy is not a static right to exclusion or a transactional commodity but a *spatio-ethical relation*—one that must be maintained through context-aware norms, technologically embedded safeguards, and intersubjective trust. It insists that ethical protections be responsive to the *gradient* of exposure: from the physically proximate and emotionally intense (e.g., gynecological examinations) to the algorithmically mediated and infrastructurally diffuse (e.g., wearables, databases, and telemedical platforms).

Moreover, by spatializing privacy in relation to both human proximity and technological infrastructure, this framework renders visible what is often structurally obscured—namely, the *invisible labor* of data governance, the *opacity* of algorithmic actors, and the *asymmetries* of access and power that mediate patient experiences [16,65]. In doing so, it not only enhances diagnostic clarity but offers a prescriptive agenda for how digital health systems should be ethically constructed and governed.

In sum, this model presents a critical corrective to conventional theories of privacy, offering a *cyber-aware, spatially grounded, and ethically nuanced* alternative that is urgently needed to navigate the challenges of 21st-century medicine.

Conclusion

The evolving landscape of digitally mediated healthcare demands a rethinking of privacy beyond the limitations of classical theories. As demonstrated through our critical review and the illustrative case of Patient X, traditional models—centered on control, boundary

negotiation, co-ownership, or contextual integrity—fall short when applied to the diffuse, persistent, and often opaque dynamics of cyberspatial interaction. These frameworks assume stable agents, bounded contexts, and a clear locus of agency—assumptions increasingly incompatible with the realities of hybrid clinical environments, wearable technologies, and telemedical infrastructures.

To address this gap, we proposed a multidimensional, zone-based model of privacy grounded in Edward T. Hall's proxemics and extended into the cyberspatial domain. This framework enables a more ethically sensitive analysis by recognizing that privacy violations differ not only in kind but in normative intensity depending on the proximity and modality of exposure. By categorizing privacy into spatial and cyberspatial dimensions—across intimate, personal, social, and public zones—we offer a robust tool for identifying, anticipating, and mitigating privacy risks in contemporary clinical practice.

Our model has practical implications across multiple domains. For healthcare professionals, it introduces a vocabulary and structure for ethically navigating patient data beyond legal compliance. For system designers, it provides guidance for embedding privacy by design tailored to different zones of vulnerability. For policy-makers, it offers a principled foundation for crafting zone-sensitive regulations that better reflect the complexities of digital health interactions.

Most importantly, this framework reorients the privacy debate from static rights and isolated consent events toward a dynamic ethics of spatial and digital co-presence. In doing so, it moves us closer to a healthcare paradigm that respects not only the content of what is shared, but the *conditions* under which sharing occurs.

In an era where the boundaries between physical and digital care are increasingly porous, privacy must be reimagined not as a barrier to innovation, but as a critical enabler of trust, autonomy, and dignity. This article contributes to that reimagining by offering both a conceptual corrective and a practical foundation for ethical design, governance, and care within digitally mediated healthcare.

Abbreviations

AI	Artificial Intelligence
EHR	Electronic Health Record
GDPR	General Data Protection Regulation
ICTs	Information and Communication Technologies
MRI	Magnetic Resonance Imaging
HIPAA	Health Insurance Portability and Accountability Act

Acknowledgements

The authors thank the reviewers for their insightful comments and suggestions, which helped improve the manuscript.

Authors' contributions

OO developed the conceptual framework, wrote the initial draft, and integrated feedback. EMD contributed to the theoretical analysis, literature review, and manuscript revisions. Both authors read and approved the final manuscript.

Funding

No funding was received for this study.

Data availability

No datasets were generated or analysed during the current study.

Declarations**Ethics approval and consent to participate**

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare no competing interests.

Received: 27 August 2025 / Accepted: 18 December 2025

Published online: 08 January 2026

References

- Lupton D. The quantified self: A sociology of Self-Tracking. Cambridge: Polity; 2016.
- Mittelstadt BD, Floridi L. The ethics of big data: current and foreseeable issues in biomedical contexts. In: Mittelstadt BD, Floridi L, editors. The ethics of biomedical big data. Cham: Springer; 2016. pp. 445–80.
- Ebeling MF. Healthcare and big data: digital specters and Phantom objects. Basingstoke: Palgrave Macmillan; 2016.
- Van Dijck J, Poell T. Understanding the promises and premises of online health platforms. *Big Data & Society*. 2016 June [cited 2025 July 23];3(1). Available from: <https://journals.sagepub.com/doi/https://doi.org/10.1177/2053951716654173>
- De Arriba-Pérez F, Caeiro-Rodríguez M, Santos-Gago J. Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios. *Sensors*. 2016 Sept 21;16(9):1538.
- Cohen JE. Configuring the networked self: Law, Code, and the play of everyday practice. New Haven: Yale University Press; 2012.
- Bak M, Madai VI, Fritzsche MC, Mayrhofer MTH, McLennan S. You can't have AI both ways: balancing health data privacy and access fairly. *Front Genet*. 2022;13:929453.
- Solove D. A taxonomy of privacy. *Univ Pa Law Rev*. 2006;154(3):477.
- Nissenbaum H. Privacy in context: Technology, Policy, and the integrity of social life. Stanford, CA: Stanford University Press; 2010. p. 1.
- Nebecker C, Torous J, Bartlett Ellis RJ. Building the case for actionable ethics in digital health research supported by artificial intelligence. *BMC Med*. 2019 Dec [cited 2025 July 23];17(1). Available from: <https://bmcmmedicine.biomedcentral.com/articles/https://doi.org/10.1186/s12916-019-1377-7>
- Morley J, Machado CCV, Burr C, Cows J, Joshi I, Taddeo M, et al. The ethics of AI in health care: A mapping review. *Soc Sci Med*. 2020 Sept;260:113172.
- Sharon T. The googlization of health research: from disruptive innovation to disruptive ethics. *Per Med*. 2016;13(6):563–74.
- Onder O. Klinik Karar Destek Sistemleri Bağlamında Tıpta Yapay Zeka Kullanımında Etik Sorun Alanları. Doctoral dissertation. Istanbul University; 2025. <https://philarchive.org/rec/ONDKKD>.
- Ohm P. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Rev*. 2010;57(6):1701–77.
- Pasquale F. The black box society: the secret algorithms that control money and information. Cambridge: Harvard University Press; 2015.
- Andrejevic M, Gates K. Big data surveillance: introduction. *Surveillance Soc*. 2014;12(2):185–96.
- Westin AF. Privacy and freedom. New York: Atheneum; 1967.
- Altman I. The environment and social behavior: Privacy, personal Space, Territory, and crowding. Monterey: Brooks/Cole; 1975.
- Petronio S. Boundaries of privacy: dialectics of disclosure. Albany: State University of New York; 2002.
- Zuboff S. The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: PublicAffairs; 2019.
- Mittelstadt BD, Allo P, Taddeo M, Wachter S, Floridi L. The ethics of algorithms: Mapping the debate. *Big Data & Society*. 2016 Dec [cited 2025 July 23];3(2). Available from: <https://journals.sagepub.com/doi/https://doi.org/10.1177/2053951716679679>
- Boyd D. Social network sites as networked publics: Affordances, dynamics, and implication. In: Papacharissi Z, editor. A networked self: Identity, Community, and culture on social network sites. 1st ed. New York: Routledge; 2011. pp. 39–58.
- Van Dijck J. Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. *SS*. 2014;12(2):197–208.
- Poster M. What's the matter with the internet? Minneapolis. University of Minnesota Press; 2001.
- Dodge M, Kitchin R. Codes of life: identification codes and the Machine-Readable world. *Environ Plan D*. 2005;23(6):851–81.
- Haggerty KD, Ericson RV. The surveillant assemblage. *Br J Sociol*. 2000;51(4):605–22.
- Andrejevic M, iSpy. Surveillance and power in the interactive era. Lawrence: University Press of Kansas; 2007.
- Lupton D. Critical perspectives on digital health technologies. *Sociol Compass*. 2014;8(12):1344–59.
- Ruckenstein M, Schüll ND. The Datafication of Health. *Annual Review of Anthropology*. 2017;46(Volume 46, 2017):261–78.
- Buhr E, Onder O, Rudra P, Ursin F. Trust and artificial intelligence in the Doctor-Patient relationship: epistemological preconditions and reliability gaps. *Ethics Inf Technol*. 2025;27(4):60.
- Bauman Z, Lyon D. Liquid surveillance: a conversation. Malden, MA: Polity Press; Cambridge, UK; 2013. p. 182. (Polity conversations series).
- Hall ET, Proxemics. *Curr Anthropol*. 1968;9(2/3):83–108.
- Hall ET. Handbook for proxemic research. Washington: Society for the Anthropology of Visual Communication; 1974.
- Floridi L. The fourth revolution: how the infosphere is reshaping human reality. Oxford: Oxford University Press; 2014.
- Guala F. The methodology of experimental economics. Cambridge: Cambridge University Press; 2005.
- van de Poel I. Translating values into design requirements. In: Michelfelder DP, McCarthy N, Goldberg DE, editors. Philosophy and engineering: reflections on Practice, principles and process. Detroit: Macmillan Reference USA; 2013.
- Castells M. The rise of the network Society. Second edition with a new preface. Oxford: Wiley-Blackwell; 2009. p. 1. (The information age).
- Ottis R, Lorents P. Cyberspace: Definition and Implications. In: Proceedings of the 5th International Conference on Information Warfare and Security. Dayton, OH, US: Reading: Academic Publishing Limited; 2010. pp. 267–70.
- Swierstra T. Identifying the normative challenges posed by technology's 'soft' impacts. *Etikk I Praksis - Nordic J Appl Ethics*. 2015;9(1):5–20.
- Van Den Hoven J. Information Technology, Privacy, and the Protection of Personal Data. In: van den Hoven J, Weckert J, editors. Information Technology and Moral Philosophy. Cambridge: Cambridge University Press; 2008 [cited 2025 July 18]. pp. 301–21. (Cambridge Studies in Philosophy and Public Policy). Available from: <https://www.cambridge.org/core/books/information-technology-and-moral-philosophy/information-technology-privacy-and-the-protection-of-personal-data/17E12096D1BA1F8E376703AFE18784FF>
- Floridi L. The ethics of information. Oxford: Oxford University Press; 2014. p. 1.
- Verbeek PP. What things do: philosophical reflections on Technology, Agency, and design. University Park: Penn State University; 2005.
- Brey P. Anticipatory ethics for emerging technologies. *NanoEthics*. 2012;6(1):1–13.
- Swierstra T, Rip A. Nano-ethics as NEST-ethics: patterns of moral argumentation about new and emerging science and technology. *NanoEthics*. 2007;1(1):3–20.
- Raybeck D. Proxemics and privacy: managing the problems of life in confined environments. In: Harrison AA, Clearwater YA, McKay CP, editors. From Antarctica to outer space: life in isolation and confinement. New York: Springer; 1991.
- Tovino SA. Functional neuroimaging and the law: trends and directions for future scholarship. *Am J Bioeth*. 2007 Sept 14;7(9):44–56.
- Hasinoff AA, Shepherd T. Sexting in context: privacy norms and expectations. *Int J Communication*. 2014;8(0):24.
- Clark JW, Snyder P, McCoy D, Kanich C, I Saw Images I. Didn't Even Know I Had: Understanding User Perceptions of Cloud Storage Privacy. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. Seoul Republic of Korea: ACM; 2015 [cited 2025 July 29]. pp. 1641–4. Available from: <https://doi.org/10.1145/2702123.2702535>
- Kupritz VW. Privacy in the workplace: the impact of Building design. *J Environ Psychol*. 1998;18(4):341–56.

50. Koops BJ, Newell B, Timan T, Skovráněk I, Chokrevski T, Galič M. A typology of privacy. *Univ Pa J Int Law*. 2017;38(2):483–575.
51. Andrews L, I Know Who You Are and I Saw What You Did. Social networks and the death of privacy. New York: Free; 2012. p. 274.
52. Barrett-Maitland N, Lynch J, Social Media. Ethics and the Privacy Paradox. In: Kalloniatis C, Travieso-Gonzalez C, editors. *Security and Privacy From a Legal, Ethical, and Technical Perspective*. IntechOpen; 2020 [cited 2025 July 29]. Available from: <https://www.intechopen.com/books/security-and-privacy-from-a-legal-ethical-and-technical-perspective/social-media-ethics-and-the-privacy-paradox>
53. Mittelstadt B. Ethics of the health-related internet of things: a narrative review. *Ethics Inf Technol*. 2017 Sept;19(3):157–75.
54. McGuire AL, Caulfield T, Cho MK. Research ethics and the challenge of whole-genome sequencing. *Nat Rev Genet*. 2008;9(2):152–6.
55. Dove ES, Joly Y, Tassé AM, Public Population Project in Genomics and Society (P3G) International Steering Committee, International Cancer Genome Consortium (ICGC) Ethics and Policy Committee, Knoppers BM. Genomic cloud computing: legal and ethical points to consider. *Eur J Hum Genet*. 2015;23(10):1271–8.
56. Eichinger J, Elger BS, Koné I, Filges I, Shaw D, Zimmermann B, et al. The full spectrum of ethical issues in pediatric genome-wide sequencing: a systematic qualitative review. *BMC Pediatr*. 2021;21(1):387.
57. Erlich Y, Shor T, Pe'er I, Carmi S. Identity inference of genomic data using long-range Familial searches. *Science*. 2018;362(6415):690–4.
58. Clayton EW, Evans BJ, Hazel JW, Rothstein MA. The law of genetic privacy: applications, implications, and limitations. *J Law Biosci*. 2019;6(1):1–36.
59. Kruse CS, Krowski N, Rodriguez B, Tran L, Vela J, Brooks M. Telehealth and patient satisfaction: a systematic review and narrative analysis. *BMJ Open*. 2017;7(8):e016242.
60. Cohen IG, Amarasingham R, Shah A, Xie B, Lo B. The legal and ethical concerns that arise from using complex predictive analytics in health care. *Health Aff*. 2014 July;33(7):1139–47.
61. Sharon T. From hostile worlds to multiple spheres: towards a normative pragmatics of justice for the googlization of health. *Med Health Care Philos*. 2021 Sept;24(3):315–27.
62. Prainsack B. Logged out: Ownership, exclusion and public value in the digital data and information commons. *Big Data Soc*. 2019;6(1):2053951719829773.
63. El Emam K, Jonker E, Arbuckle L, Malin B. RW <>Scherer editor 2011 A systematic review of Re-Identification attacks on health data. *PLoS ONE* 6 12 e28071.
64. Alder S. Healthcare Data Breach Statistics. *The HIPAA Journal*. 2025 [cited 2025 July 21]. Available from: <https://www.hipaajournal.com/healthcare-data-breach-statistics/>
65. Dastin J. Amazon scraps secret AI recruiting tool that showed bias against Women *. *Ethics of data and analytics*. Auerbach; 2022.
66. Tene O, Polonetsky J. Big data for all: privacy and user control in the age of analytics. *Northwest J Technol Intellectual Property*. 2013;11(5):239.
67. Wang Y, Kung L, Byrd TA. Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technol Forecast Soc Chang*. 2018;126:3–13.
68. Rumbold JMM, Pierscionek B. The effect of the general data protection regulation on medical research. *J Med Internet Res*. 2017;19(2):e7108.
69. Barocas S, Nissenbaum H. Big data's end run around procedural privacy protections. *Commun ACM*. 2014;57(11):31–3.
70. Van Den Hoven J, Vermaas PE, Van De Poel I, editors. *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains*. Dordrecht: Springer Netherlands; 2015 [cited 2025 July 29]. Available from: <https://link.springer.com/> <https://doi.org/10.1007/978-94-007-6970-0>
71. Petersen A, Munsie M, Tanner C, MacGregor C, Brophy J. *Stem Cell Tourism and the Political Economy of Hope*. London: Palgrave Macmillan UK; 2017 [cited 2025 July 29]. Available from: <http://link.springer.com/> <https://doi.org/10.1057/978-1-137-47043-0>
72. Hendl T, Shukla A. Can digital health democratize health care? *Bioethics*. 2024 July;38(6):491–502.
73. Lidströmer N, Davids J, ElSharkawy M, Ashrafian H, Herlenius E. A summit on a global patient co-Owned cloud (GPOC). *BMC Digit Health*. 2024;2(1):51.
74. Davids J, ElSharkawy M, Ashrafian H, Herlenius E, Lidströmer N. Technical sandbox for a global patient co-Owned cloud (GPOC). *BMC Digit Health*. 2024;2(1):75.
75. Lidströmer N, Davids J, ElSharkawy M, Ashrafian H, Herlenius E. Necessity for a global patient co-owned cloud (GPOC). *BMC Digit Health*. 2024;2(1):76.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.