Journal of Electronic Research and Application, 2026, Volume 10, Issue 7
http://ojs.bbwpublisher.com/index.php/JERA
Online ISSN: 2208-3510
Print ISSN: 2208-3502

Data Privacy and Patient Consent in Smart Hospitals over the Past Decade

Tongxing Zheng, Lin Zhang

Information Center, The Second Affiliated Hospital of Wenzhou Medical University, Wenzhou, Zhejiang, China

Abstract: Over the past decade, the construction of data-driven smart hospitals has profoundly changed the medical service model and has also made data privacy and patient informed consent core ethical and legal issues. This study systematically sorts out the practical evolution of data privacy protection and informed consent in smart hospitals from 2016 to 2026, reveals the structural tension of "advanced technology and lagging system", and finds that informed consent is falling into the dilemma of scene generalization and formalization, data ownership is still pending in the legal ambiguity zone, and technical governance brings privacy risks while improving efficiency, forming a "double-edged sword" effect. On this basis, the study puts forward that the key to break through the dilemma lies in the transition from "one-time authorization" to "dynamic informed consent" mechanism, the construction of a three-dimensional protection framework of "legal regulation-technical guarantee-collaborative governance", and the promotion of institutional innovation in data rights confirmation and benefit distribution; only by putting patients at the center of data governance can we maintain the ethical bottom line in the digital transformation of medical care.

Keywords: Smart hospital; Data privacy; Informed consent; Patient's rights; Data governance

Online publication: Aug 13, 2026

1. Introduction

Smart hospital is not a sudden concept. Over the past decade, on the one hand, the widespread popularity of electronic medical records and the gradual implementation of artificial intelligence-assisted diagnosis and treatment, on the other hand, the entry of wearable devices into the clinic and the real-time recording of doctor-patient dialogue by 'environmental clinical AI', these changes have gradually brought the digital transformation of medical services from the original vision into daily reality [1]. The core driving force of this profound transformation is data. If the collection, circulation, and training of massive health data are missing, smart medical care will completely lose its foundation and be impossible to talk about [2].

However, it is precisely this set of 'data-driven' logic that pushes patient privacy protection to unprecedented challenges [3]. Medical and health information has been clearly classified into the category of "sensitive personal information" defined in Article 28 of the Personal Information Protection Law. Once

it is leaked or abused, it is likely to bring immeasurable damage to the patient's life, social evaluation, and even personal dignity. On the other hand, the patient's informed consent, the core principle of traditional medical ethics, has also fallen into a crisis of applicability in the context of smart hospitals: the use of data is expanding, and the circulation chain has become increasingly complex. The practice of "one-time notification and one-time signature" has been difficult to truly achieve full informed and independent choice [4].

This paper mainly reviews the practical evolution and institutional response of data privacy and patients' informed consent in the context of smart hospitals in the past decade, analyzes the core dilemmas, and discusses the future-oriented optimization path [5]. The core argument of the research is that the data governance of smart hospitals must not be at the expense of patient autonomy, and the construction of a dynamic, layered, and traceable informed consent mechanism and data protection system is an unavoidable ethical bottom line in the process of medical digital transformation.

2. The problem of data privacy in smart hospitals is proposed

In the past ten years, China's rule of law construction in the field of medical data governance has gone through an evolution process from weak to gradual formation. On the one hand, in the early stage (2016–2020), the construction of smart hospitals has advanced rapidly, but the norms of data protection have lagged; although the "Medical Record Management Regulations for Medical Institutions" issued in 2018 involves medical record management, it lacks response to new problems such as secondary use of data and cross-border flow [6]. During this period, patients' health data are often regarded as "hospital assets" in practice, and informed consent is also a mere formality. On the other hand, after entering the period of intensive system construction (2021–2023), the 'Data Security Law' (2021) and 'Personal Information Protection Law' (2021) have been implemented one after another, bringing medical data governance into the track of rule of law; in particular, the 'Personal Information Protection Law', for the first time at the legal level, establishes 'informed consent' as the core legal basis for the processing of sensitive personal information, and clearly requires that the processing of medical and health information must obtain the individual's 'individual consent'. The "Measures for the Administration of Network Security in Medical and Health Institutions" issued in 2022 further established systems such as data hierarchical protection and data security subject responsibility, while the "National Medical and Health Institutions Information Exchange and Sharing Three-Year Action Plan (2023–2025)" launched in 2023 put forward higher requirements for data security while promoting data sharing [7].

After entering the period of improvement and deepening (2024–2026), the focus of legislation has obviously shifted from "with or without" to "fine". Academics and practitioners generally call for further refinement of medical data classification standards and the establishment of dynamic authorization mechanisms. In 2025, Beijing launched a technical specification for the anonymization of health care data, which provides operational guidance for 'data available and unidentifiable'; the " Expert Consensus on the Application and Governance of Artificial Intelligence in Medical Institutions (2026) issued in 2026, systematically proposed the governance framework of hierarchical informed consent and algorithmically interpretable response for the first time [8].

In general, China has initially established a data protection system covering laws, administrative regulations, departmental rules, and technical standards. However, the transformation of the system from "existing" to "excellent" is still on the way, and the tension between legal norms and technological

development has not been fundamentally resolved.

The deep root of this tension is the structural contradiction between the inherent lag of legislation and the acceleration of technological iteration. The special feature of medical data governance is that the object it regulates–health information is not only sensitive personal information that needs strict protection in the legal sense, but also the core production factor that drives artificial intelligence model training, clinical decision support system optimization, and precision medicine research. From drafting, deliberation, to final promulgation and implementation, a legal norm often takes years, and the technology associated with it is likely to have completed multiple iterations and upgrades during this cycle; the protection framework set by the legislation at that time, by the time the technology really landed, it may have been necessary to face the new risk form.

Specifically, this tension is particularly evident in the following three dimensions.

The first dimension is the dilemma of legal concepts in the face of technology adaptation. The "Personal Information Protection Law" defines "anonymization as the state in which personal information cannot be identified as a specific natural person and cannot be restored after processing, and stipulates that the information after anonymization no longer belongs to personal information and can be freely used. This legal definition takes non-recoverability as the only criterion, which seems clear on the surface, but actually shifts the huge burden of judgment to technical practice. At present, there has been a heated debate about the reliability of anonymization technology in the academic community. Some studies have pointed out that even after a seemingly sufficient de-identification process, specific individuals can still be re-identified with a high probability by cross-matching multiple public data sets. With the continuous improvement of correlation analysis technology and artificial intelligence inference ability, today's 'unrecoverable' data is likely to become 'recoverable' by tomorrow. Using a set of static standards to regulate the dynamic evolution of technology, its effectiveness will inevitably continue to encounter challenges.

The second dimension is the coverage gap between normative supply and governance demand. The data circulation of smart hospitals is increasingly showing the characteristics of cross-agency, cross-region, and cross-boundary, while the current institutional framework still regards "institution-based" as the basic logic, that is, medical institutions are used as data controllers to set compliance obligations. However, in the medical big data industry ecology, the actual flow path of data often involves multiple entities such as cloud service providers, data analysis companies, AI algorithm developers, and drug research and development companies. Once the data leaves the medical institution, how can the patient's right to know, delete, and withdraw consent rights be effectively guaranteed among multiple entities? The current norms have not given a clear answer. This institutional feature of "strict control at the front end and out of focus at the back end" will make the protection system have an obvious coverage vacuum in the middle and lower reaches of the data circulation chain.

The third dimension is the realistic imbalance between compliance costs and innovation incentives. Strict data protection regulations will inevitably lead to an increase in the compliance costs of medical institutions and technology companies; for large tertiary hospitals, it is still affordable to establish a complete privacy protection compliance system, but for primary medical institutions and start-up digital health enterprises, complicated compliance requirements may constitute substantial barriers to entry. System design must face such a balance problem: how to avoid excessive regulation while protecting patients' privacy rights, so as to inhibit the value release of medical data elements and the innovative development of the artificial intelligence

industry. The "Guiding Opinions on Promoting and Regulating the Circulation of Medical and Health Data Elements" issued in 2025 clearly put forward the principle of "Inclusive Prudential Supervision", which can be regarded as an institutional response to this balanced appeal. However, the specific implementation effect of this principle needs to be further tested by practice.

3. The practical dilemma and institutional reflection of the principle of informed consent

Informed consent is the institutional carrier of patient autonomy and the most vulnerable link in data governance of smart hospitals.

3.1. Formal crisis of informed consent

In traditional medical scenarios, informed consent has always been aimed at specific diagnosis and treatment behaviors, with clear objectives and clear boundaries. However, in smart hospitals, a patient's visit may involve many different data uses, such as electronic medical record entry, AI-assisted diagnosis, clinical research contribution, hospital management analysis, etc [9]. The current practice often adopts 'packaged authorization', and all multiple scenarios are included in a formatted consent form. Patients face lengthy terms, either signing in exchange for services, or giving up - this 'do not accept that exit' structure makes it difficult for consent to be regarded as a real voluntary choice, and ultimately reduces it to a poll-based form of authorization [10].

In the face of this dilemma, 'dynamic informed consent' has been proposed as an alternative. It allows patients to continuously adjust the scope of authorization according to different scenarios, purposes, and stages of data use, and can withdraw consent at any time. For example, a patient may be willing to use his de-identified data for drug development of a specific cancer, but will refuse to authorize it to a commercial insurance agency for risk assessment. The "Expert Consensus on the Application and Governance of Artificial Intelligence in Medical Institutions" issued in 2026 has clearly stated that "hierarchical informed consent" should be implemented according to the risk level of AI applications–low-risk applications can adopt informed consent, and high-risk applications need to obtain special written consent. To make dynamic consent truly landed, it is inseparable from technical support. Blockchain, self-sovereign identity, de-identified tokens, and other technologies are being explored to build an auditable and traceable consent management system.

However, it must be recognized that informed consent itself does not solve all problems: on the one hand, the law allows exemptions from informed consent in scenarios such as public health emergencies; on the other hand, when the data is fully anonymized, the use does not require separate authorization, however, whether the 'anonymized' technical standards are reliable and whether they can withstand the challenges of reverse identification of future technologies is always an open question. See **Figure 1**.

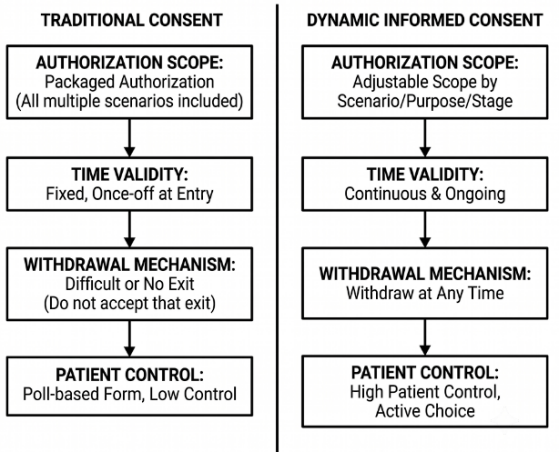

Figure 1. Comparison of traditional consent and modified consent. Dynamic informed consent.

3.2. Blurred areas of data ownership

Patients often subconsciously believe that their health data should be 'their own', but the situation in legal practice is far from so simple. The current framework is the 'separation of three rights', which is divided into three levels: First, patients have personal rights and interests in personal information (including informed, corrected, deleted, etc.); secondly, the medical data formed by medical institutions based on diagnosis and treatment services enjoy the 'data resource holding right' and 'processing and using right'. Third, third-party institutions are authorized to enjoy 'data product management rights'. Although this framework attempts to balance the interests of multiple parties, the differences in the legal nature of 'rights' and 'rights', the boundaries and conflicts of rights of all parties still need to be further clarified through judicial practice.

Associated with the problem of ownership, there are also problems in the distribution of benefits. Health data is becoming an asset with great economic value. The 'Xihe No.1 Medical Model' released in 2025 is based on the training of 1 million real medical records of 18 institutions. When these data are used for commercial purposes (such as pharmaceutical research and development, AI model training), should patients benefit from them? At present, it has been proposed to establish a 'patient equity fund', with no less than 5% of the proceeds from data transactions dedicated to patient subsidies and privacy protection research and development. Although this mechanism is still in the exploratory stage, this direction is worthy of recognition - the value creators of data cannot be excluded from the value distribution. See **Figure 2**.

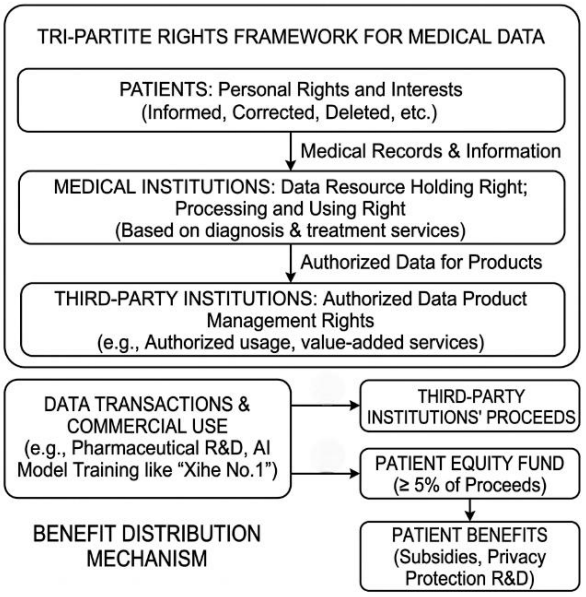

Figure 2. Tripartite rights framework and benefit distribution mechanism.

3.3. The duality of technical governance

In the process of data governance in smart hospitals, the application of technology shows the dual characteristics of protection and risk.

From the perspective of privacy risk, the rapid promotion of environmental clinical AI (i.e., 'listening AI') has aroused widespread concern. Such systems record doctor-patient conversations and generate medical records in real time through an always-on microphone. Although it has a significant effect on reducing the burden of doctors' paperwork (some studies have shown that it can reduce document time by 20–30%), patients are likely to be recorded 'unintentionally' because of their continuous voice collection; studies have shown that many patients are unaware of the existence of these systems and even less aware of where the data is going. See **Table 1**.

Table 1. Ambient clinical AI ("Listening AI") privacy risk data

Dimension	Indicator	Data
Clinical benefit	Reduction in physician documentation time	20–30%
	Usage in large health system (14 months)	7,000+ clinicians, 2.5M+ patient encounters
	Adoption rate at academic medical center (2 years)	44.6% (1,565 outpatient physicians)
Patient awareness	Patients unfamiliar with ambient AI	77.9% (n = 462 patient survey)
	Aware patients who felt uncomfortable	0.394
	Patients believing AI improved visit quality	56–84%
Informed consent	Physician explanation associated with greater comfort	OR = 2.32 (95% CI 1.49–3.61)
Data security	Institutions ranking data security as top concern	53% (survey of 36 research sites)
	Patient privacy ranked as top AI ethics priority	Tied with "algorithmic fairness" as highest
Data flow	Voice data involving third-party cloud storage	Mainstream products rely on cloud processing
	Patient unawareness of data destination	Widespread lack of transparency

Data Sources: Patient awareness data (77.9% unfamiliar, 39.4% discomfort): Cross-sectional survey of 462 patients reported at AMIA 2026 Annual Symposium; Clinical benefit (20–30% time reduction): Nature npj Digital Medicine review; JMIR Systematic Review reports 22%; Institutional concern (53% data security): NIH-funded environmental scan across 36 research sites

In the dimension of privacy protection, blockchain technology provides technical possibilities for data authentication and authorization traceability; federated learning enables AI models to achieve training without centralized collection of raw data, so that 'data is not visible'; trusted data space and privacy computing technologies are also being gradually introduced into the scenario of medical data sharing. The deep challenge of technical governance is that the development of solutions often gives priority to functional efficiency, and privacy protection functions are easily regarded as add-ons without becoming the core elements of system design. The 2026 expert consensus clearly stated the requirement of 'algorithmic interpretability', when patients have objections to the results of AI-assisted diagnosis, medical institutions have an obligation to provide visual evidence and explain it, which is an attempt to truly embed patient rights into the technical system.

4. Conclusion

In the past decade, while making medical services more intelligent and efficient, smart hospitals have also shaped data privacy and informed consent of patients into an unavoidable governance problem. Technology has the ability to assist in diagnosis and optimize processes, but it cannot replace respect for patient autonomy. As medical digitization moves into the next decade, what is needed is not only smarter algorithms, but also more robust systems, more transparent governance, and the kind of ethical consciousness that truly puts patients at the center of data governance. Only in this way can smart hospitals be worthy of the word "wisdom" - its wisdom is not only in the wisdom of technology, but also in the wisdom of the system and the wisdom of the people.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Lenz E, Naamanka J, Trabert W, et al., 2026, Benchmarking Large Language Models Against Practicing Clinicians on Psychopathological Assessment. npj Digital Medicine, 9(1): 1–12.

[2] O'Neill S, DesRoches C, 2025, How Should We Think About Ambient Listening and Transcription Technologies' Influences on EHR Documentation and Patient-Clinician Conversations? AMA Journal of Ethics, 27(11): E780–E786.

[3] Khan I, Smith L, 2025, What Are Ethical Merits and Drawbacks of a Patient's Open and Direct Access to Clinical Information in Their EHRs During a Hospital Stay? AMA Journal of Ethics, 27(11): E774–E779.

[4] Roberts J, 2025, How Could Legal Standards Promote Equitable Access to EHRs? AMA Journal of Ethics, 27(11): E815–E820.

[5] Bendjeddou A, Zeinalipour K, Bardou D, et al., 2026, PharMistral: Drug Generation for Novel Protein Targets by Mistral Large Language Model. Computer Methods and Programs in Biomedicine Update, 10: 100257.

[6] Al-Dolat W, Alhatamleh S, Malkawi M, et al., 2026, DenseWave-OCT: A Hybrid Deep Learning and Wavelet Scattering Framework for Multi-Class Retinal Disease Classification in Optical Coherence Tomography Images. Computer Methods and Programs in Biomedicine Update, 10: 100260.

[7] Iqbal M, Alyatimi A, Chung V, et al., 2026, Advances in AI-Driven Image Analysis for Sarcoma Diagnosis: A Comprehensive Scoping Review. Computer Methods and Programs in Biomedicine Update, 10: 100259.

[8] Gu J, Uthamacumaran A, Zenil H, 2026, A Review of Point-of-Care Devices for Blood-Testing Towards AI-Driven Remote Digital Care, Precision Healthcare and Predictive Medicine. Computer Methods and Programs in Biomedicine Update, 10: 100258.

[9] Gebreab S, Musamih A, Salah K, 2026, An LLM-Based Multi-Agent System for Patient Discharge Assessment. Computer Methods and Programs in Biomedicine Update, 10: 100261.

[10] Rinaldi E, Kush R, Dalmiani S, 2026, Editorial: Unlocking the Potential of Health Data: Interoperability, Security, and Emerging Challenges in AI, LLM, Precision Medicine, and Their Impact on Healthcare and Research. Frontiers in Digital Health, 8: 1783831.