REVIEW
UDC: 614.253.8(430)
614.253.8 497.2)
614.253.8(497.7)
614.253.8(510)

Health data protection and patient safety in Germany, Bulgaria, North Macedonia and China

Mihail Mihaylov[1,3] Orcid ID 0009-0001-3673-7392
Kire Stojkovski[2] Orcid ID 0000-0002-9903-0036
Stanislav Malchev[3] Orcid ID 0009-0009-5495-7063

1 Medical Center OBLIQ, Sofia, Bulgaria
2 PSI-CRO – Sofia, Bulgaria
3 Faculty of Public Health "Prof. Dr. Tzecomir Vodenitcharov", Medical University of Sofia, Bulgaria

Article received: 14.09.2026
Article revised: 18.09.2026
Article accepted: 22.09.2026

DOI: https://www.doi.org/10.59710/oaijoaru264349pm

Abstract

This review compares personal health information protection in Germany, Bulgaria, North Macedonia, and mainland China, emphasizing patient safety, biomedical research, and digital health services. Comparative legal analysis and a narrative review examined legislation, judgments, regulatory guidance, and five scholarly publications retrieved by September 24, 2026. Analytical categories included lawful processing, confidentiality, patient access, research, supervision, international transfers, and product requirements. Germany and Bulgaria share the General Data Protection Regulation but differ in sectoral implementation. North Macedonia illustrates European legal approximation, including distinctive prior-approval requirements and transfer concerns. China combines sensitive-information safeguards with network data governance and additional controls on human genetic resources. Similar terminology does not imply equivalent institutions or transfer permissions. The European Health Data Space adds phased obligations, requiring separation of current compliance from future preparedness. Clinical literature supports attention to record accuracy, understandable patient access, and trustworthy research, without establishing comparative national health outcomes. Recommended practices include purpose-specific governance, traceable access, appropriate impact assessments, accessible correction procedures, and separate review of research and cross-border requirements. Public benefit depends on whether confidentiality, accuracy, and lawful availability jointly support safe care, equitable participation, and accountable knowledge generation.

Keywords: health data; patient safety; digital medicine; comparative law; health policy

1 Introduction

Personal health information supports diagnosis, continuity of care, quality assessment, and health-system planning while revealing intimate aspects of a person's life. Its protection therefore encompasses confidentiality, accuracy, availability, and lawful exchange. Unauthorized disclosure can cause stigma and undermine trust; withholding necessary information can also create clinical risk. Data protection is consequently a component of healthcare quality, rather than a purely administrative obligation [1, 2].

Under Article 4(15) of the General Data Protection Regulation (GDPR), health data concern physical or mental health, including healthcare provision, and reveal health status. Protection is not determined by whether information resides in a hospital record, laboratory system, or application. Genetic data constitute a separate special category; biometric data receive special-category protection when processed to identify a person uniquely. Pseudonymization generally leaves data within the regulatory framework, whereas genuine anonymization requires consideration of identification by reasonably likely means [1].

Comparing two European Union (EU) Member States with a candidate country distinguishes common rules, national implementation, and pre-accession approximation. Mainland China provides a fourth, autonomous regulatory model; it is not analyzed as an EU candidate. Hong Kong, Macao, and Taiwan are outside scope. The objective is to identify shared safeguards and consequential differences, and to derive recommendations for clinical organizations, regulators, and digital health providers. The central question is how these regimes reconcile confidentiality with treatment, research, and technological development. Particular attention is given to whether legal convergence creates usable rights and socially valuable data use.

2 Materials and methods

This study uses comparative legal analysis, functional comparison, and a narrative review of documentary sources. Searches covered EUR-Lex, European court resources, the German Gesetze im Internet portal, health ministries, national data protection authorities, European Commission publications, Chinese legislative and regulatory portals, and publisher or bibliographic pages for scholarly literature. Search concepts in Bulgarian, German, Macedonian, Chinese, and English concerned medical confidentiality, health data, patient records, secondary use, and trust. The retrieval cutoff was September, 2026.

Selection was purposive. Included sources directly regulated or explained the selected mechanisms, or synthesized evidence relevant to patient access and responsible sharing. The corpus comprises legislation, judgments, institutional guidance, and five scholarly publications: three systematic reviews, one patient survey, and one technical review. This article is not a systematic review of all available legal or medical literature. Analysis used common categories: legal hierarchy, lawful processing, secrecy, access,

supervision, transfers, research use, and digital market requirements. Binding rules, adopted provisions with deferred application, institutional assessments, and the recommendations developed here were distinguished.

The study examined public documents and published research; it involved no participant recruitment, intervention, or identifiable patient-level data. Institutional consolidated legal texts were considered alongside identified amendments. Differences in consolidation dates and the absence of an exhaustive legislative audit limit conclusions about completeness, as discussed in Section 3.9.

3 RESULTS AND DISCUSSION

3.1 European framework

The EU Charter distinguishes respect for private life under Article 7 from the right to personal data protection under Article 8. Article 35 situates healthcare within the same fundamental-rights framework, subject to Article 51 on the Charter's scope. Health policy must reconcile legitimate information use with proportionality and independent oversight [3]. The European Convention on Human Rights is a Council of Europe instrument and also applies to North Macedonia. In I. v. Finland, the European Court of Human Rights found inadequate practical protection of hospital records. The possibility of subsequent compensation did not replace effective preventive safeguards [2].

In Germany and Bulgaria, processing health data ordinarily requires both an Article 6 GDPR basis and an applicable Article 9 exception. Article 9(2)(h) addresses necessary processing for diagnosis, care, and management of health services under its legal conditions and professional-secrecy safeguards. Public health and research are addressed separately by Article 9(2)(i) and (j). A contract with a technology provider or reliance on legitimate interests alone does not remove the special-category prohibition [1].

Consent to treatment and consent to data processing are distinct legal acts. Lawfully regulated care does not universally require a separate GDPR consent form. Bulgaria's Commission for Personal Data Protection explains circumstances in which consent is unnecessary. Conversely, using treatment photographs for advertising introduces a separate purpose requiring its own legal assessment [1, 4].

Access, rectification, restriction, erasure, and portability have different conditions. Mandatory retention can limit erasure, and portability does not apply to every processing operation. In FT v. DW, Case C-307/22, the Court of Justice of the European Union confirmed the right to a first free copy of personal data in medical records without requiring the patient to justify the request. Complete documents must be supplied where necessary to make the data intelligible, while other persons' rights remain relevant [5].

Accountability requires demonstrable safeguards. Articles 25, 28, 30, 32, and 35 GDPR address design, processors, processing records, security, and impact assessment.

Notification to the supervisory authority is generally required within 72 hours of awareness unless a breach is unlikely to result in risk. Communication to affected individuals has a separate high-risk threshold. Obligations concerning data protection officers depend on applicable criteria, including large-scale processing of special categories; identical duties should not be assumed for every medical practice [1].

Regulation (EU) 2025/327 establishes the European Health Data Space (EHDS), supplementing the GDPR through rules on primary use, secondary use, and electronic health record systems. Entry into force on March 26, 2025 did not make every mechanism immediately applicable. The general application date is March 26, 2027, with major operational requirements phased into 2029 and 2031. These phases cover priority categories for exchange and secondary-use arrangements [6, 7].

For secondary use, the EHDS provides controlled access for specified purposes, secure processing environments, and an opt-out mechanism under Article 71, subject to regulated exceptions. Prohibited purposes include advertising and marketing and specified detrimental decisions about individuals. Commercial participation in permitted research must therefore be distinguished from unrestricted commercialization of patient records. The phased timetable is central to policy planning: future duties should neither be described as already fully applicable nor ignored in current system design [6].

3.2 Germany

The Federal Data Protection Act (BDSG) supplements the GDPR within the scope available to national legislation. Section 22 regulates special-category processing for healthcare and other protected purposes and identifies safeguards such as access restrictions, encryption, pseudonymization, and retrospective verification. Section 27 permits research processing without consent subject to necessity, a substantial predominance of the processing interest, and safeguards. Research is not generally exempt from protection [8].

Section 203 of the Criminal Code protects professional secrets, including those held by medical professionals, and addresses certain assisting persons involved in outsourced services. GDPR compliance does not automatically resolve whether disclosure is permissible under professional-secrecy law. Protection can continue after death [9]. The regime also includes federal and state responsibilities and institution-specific requirements. This review addresses the federal core rather than treating all state hospital laws as identical.

Access to treatment records under Section 630g of the Civil Code operates alongside the GDPR. The current text of Section 630g(1) expressly provides a first copy free of charge. The European judgment clarifies the complementary GDPR entitlement [10, 5]. The electronic patient record, or ePA, is grounded in Social Code Book V, including Section 341. The “ePA for all” model provides an opt-out mechanism; it does not grant every health professional unrestricted access. Information, access management, and

practical opportunities to exercise choice remain distinct requirements. Ministry guidance also describes objections to research use and assistance through insurers' ombuds offices for people who do not use digital channels [11, 12, 13].

The Health Data Use Act (GDNG) organizes data use for public-interest research and health-system development. It addresses coordination of access, linkage of specified datasets, supervision of research across states, secondary processing for quality and safety, secrecy, and public availability of research results. Its policy significance lies in linking facilitated access with accountability for resulting knowledge. The statutory design is informative, but does not itself demonstrate improved clinical outcomes [14].

3.3 Bulgaria

Article 32 of the Constitution protects private life. The GDPR, the Personal Data Protection Act, and health legislation provide the operational framework. The national data protection statute establishes institutional arrangements, including the supervisory commission. The Health Act contains specific provisions on health information and documentation and recognizes patients' entitlement to protection of health data [15, 16, 17].

Articles 27 and 28 address health information and disclosure to third parties in specified circumstances, including continuation of treatment and defined public needs. Article 28b governs patient access and access by specified relatives and heirs after death. These rules operate together with the GDPR: disclosure requires verification of the recipient, legal basis, purpose, and necessary scope. Kinship alone does not establish unrestricted access to a living adult's record, and technical access does not establish legal entitlement [1, 17].

Ordinance No. N-6 of December 21, 2022 regulates the National Health Information System (NHIS), including electronic records, exchange, access, and security. National infrastructure translates general rights into operational arrangements, but does not displace each provider's responsibility for its own processing, users, and local copies. Roles must follow actual functions and legislation [1, 18].

A 2026 ministerial response concerning record continuity after full adoption illustrates the interaction between confidentiality and information quality. It identifies a need to amend the ordinance to support record updates while protecting secrecy concerning origin. The response evidences an identified problem and proposed direction, rather than proving that the proposed amendment had been enacted [19]. The case shows why restricting disclosure must be reconciled with preserving an accurate clinical history.

Preparation for the EHDS requires coherent patient access, reliable identification, interoperable exchange, and secondary-use procedures. The policy recommendation arising here is to assess preparedness through practical performance: successful access to records, correction of errors, traceability, and inclusion of people with limited digital

skills. These are proposed evaluation priorities, not a claim that a particular national program has already achieved them [6, 18].

3.4 North Macedonia

The 2020 Law on Personal Data Protection adopts major GDPR-like concepts, including processing principles, lawful grounds, special categories, individual rights, impact assessment, and independent supervision. Article 13 addresses special categories, Article 19 access, and Articles 36–39 security, breaches, and impact assessment. The 2021 and 2025 amendments must be considered alongside the base text [20, 21, 22].

This is national reception of European rules, rather than general direct application of the GDPR through EU membership. Particular operators may nevertheless fall within Article 3 GDPR, for example when offering services to individuals in the Union under the specified conditions. Europeanization must be assessed through legislative content, sectoral coherence, and implementation capacity [1, 20, 23].

The Law on the Protection of Patients' Rights provides access to records, explanation of their content, and updating with preservation of original entries under Article 22. Article 25 protects confidentiality after death and limits disclosure to the relevant purpose [24]. A distinctive feature of the general data protection law is Article 84, which requires prior approval for specified processing of health, genetic, and biometric data. Paragraph 1 excepts specified genetic-data processing by experts for preventive medicine, diagnosis, care, or treatment. Paragraph 3 also excepts processing determined by law with safeguards. Outside applicable exceptions, explicit consent alone does not remove prior approval. Neither universal licensing of medical activity nor wholesale transplantation of the EU accountability model accurately describes this provision [20].

A further issue concerns the relationship between the patient-rights rule on copies charged at actual cost and the general data-protection right to a copy. Coherent interpretation should consider the precise request. Case C-307/22 is a useful European reference, but is not automatically binding in every domestic Macedonian dispute. Express clarification of free first access would support legal approximation and reduce financial barriers [5, 20, 24].

The 2025 amendment added NATO countries to transfer provisions in Articles 48 and 56. The European Commission's 2025 report criticized adoption without prior consultation with the supervisory agency and without a framework ensuring GDPR-equivalent protection. It also identified resource and staffing constraints. These findings concern the report's assessment period and should not be treated as a complete description of institutional circumstances in September 2026 [22, 23].

North Macedonia was absent from the Commission's adequacy list examined for this review. Transfers from Germany or Bulgaria consequently require an applicable Chapter V GDPR mechanism, rather than being treated as exchanges within the European

Economic Area. Contractual safeguards and supplementary measures must be considered where relevant. NATO membership is not an EU adequacy decision [1, 25]. The national agency's security, impact-assessment, and breach-notification instruments, together with its 2025–2030 strategy, support implementation. Their practical effect depends on resources and enforcement. Approximation is not necessarily linear: individual amendments can increase divergence from the acquis [23, 26, 27].

3.5 China (People's Republic of China)

The Personal Information Protection Law (PIPL), effective November 1, 2021, places medical and health information within sensitive personal information. Articles 28–30 require necessity, a specific purpose, and strict safeguards. Separate consent must be read with Article 13, which recognizes non-consent grounds; it is not universally required for every health-related operation. PIPL rights include access, copying, correction, and conditional deletion. Article 55 requires prior impact assessment for sensitive-information processing and other specified activities, including overseas provision. The statutory “personal information processor” determines purposes and methods, broadly corresponding to a GDPR controller [28].

Civil Code Article 1225 requires proper maintenance of medical records and timely access and copying on request; Article 1226 protects patient privacy and personal information through confidentiality and tort liability. These provisions connect information governance directly to the clinical relationship [29]. PIPL Article 60 assigns coordination to the national cyberspace administration and responsibilities to competent departments. This differs institutionally from the EU model of independent supervisory authorities [1, 28].

The Network Data Security Management Regulations, effective January 1, 2025, add organizational and technical requirements, including access controls, authentication, encryption, and backup. Sensitive personal information and “important data” are distinct legal categories; clinical sensitivity does not itself establish every important-data obligation [30].

The 2024 cross-border provisions differentiate exemptions, contractual or certification routes, and security assessment. For non-critical-infrastructure operators, exports involving fewer than 10,000 persons' sensitive information since January 1 generally require a standard contract or certification, whereas 10,000 or more trigger security assessment, subject to applicable exceptions and important-data rules. The small-volume exemption for ordinary personal information excludes sensitive information. Consequently, neither a blanket export ban nor unrestricted export with consent accurately describes the framework [31]. Transfers from the EU to China independently require a GDPR Chapter V basis; China is not on the reviewed EU adequacy list [1, 25].

Human genetic resources have an additional regime. The 2019 regulations, amended in 2024, govern biological materials and information derived from them, with ethics,

consent, foreign cooperation, and external-information requirements. Routine clinical activity must be distinguished from regulated research. Foreign participation in research can require Chinese cooperation and authorization; qualifying clinical trials for Chinese marketing authorization have a filing exception where materials do not leave China. Selling human genetic resources is prohibited, while specified reasonable research costs are distinguished from sale [32]. The National Health Commission's May 2026 consultation on implementing rules is treated here as a draft, not proof of enacted obligations [33].

China therefore illustrates overlapping patient-rights, data-security, and biomedical-research controls. Patient consent alone cannot substitute for every institutional or cross-border requirement. The comparative policy question is whether these controls deliver proportionate protection and accountable research; this documentary study does not measure their clinical effectiveness.

3.6 Comparative findings

The shared core comprises heightened protection of health data, patient rights, lawful exceptions, and organizational accountability. The principal differences concern operational mechanisms: authorization of new uses, coordination of secrecy and access, safeguards for international transfers, and evidence of public benefit. Table 1 summarizes these distinctions without ranking actual security performance.

Table 1. Comparison of legal mechanisms and policy priorities

Country	Patient safeguards	Research and transfers	Governance priority
Germany	GDPR; secrecy; free first record copy; ePA choice	BDSG and GDNG; phased EHDS; GDPR transfers	Coordinate federal and state rules
Bulgaria	GDPR; Health Act access; NHIS controls	Sectoral grounds; phased EHDS; GDPR transfers	Record accuracy and accessible patient procedures
North Macedonia	National rights; Article 84 approval with exceptions	Domestic transfer rules; EU transfers require Chapter V basis	Acquis alignment and supervisory capacity
China (PRC)	PIPL; clinical confidentiality; specified prior impact assessments	Export mechanisms; additional human genetic resources controls	Coordinate data and biomedical regulation

Source: comparative synthesis of the instruments discussed in Sections 3.1–3.5. GDPR, General Data Protection Regulation; EHDS, European Health Data Space; BDSG, Federal Data Protection Act; GDNG, Health Data Use Act; NHIS, National Health Information System; PIPL, Personal Information Protection Law; ePA, electronic patient record.

National law remains important after death because the GDPR does not generally govern deceased persons' data. German professional secrecy, Bulgarian access rules, Macedonian patient-rights legislation, and PIPL Article 49 on relatives' exercise of specified rights demonstrate why death does not make a medical record freely available [1, 9, 17, 24, 28].

The comparison also distinguishes legal membership from approximation. Germany and Bulgaria implement an evolving acquis within the EU legal order. North Macedonia must align domestic institutions and sectoral rules with a framework that continues to develop. China shares several functional safeguards but is not undergoing accession-driven Europeanization. Formal resemblance is an incomplete indicator of equivalence; institutional independence, transfer controls, and practical rights require separate assessment [6, 23, 28].

3.7 Digital health products and market access

Health information is not placed on the market under a general authorization scheme analogous to that for medicines. The market question concerns software, record systems, telemedicine, and research services processing such information. Three assessments must be separated: lawful processing, product conformity, and reimbursement eligibility [1, 6, 34].

In Germany and Bulgaria, software qualifying as a medical device by its intended purpose falls within Regulation (EU) 2017/745. Not every health application is a medical device. Medical-device conformity does not authorize arbitrary data use, while GDPR compliance does not demonstrate clinical safety. The EHDS adds phased requirements concerning harmonized components of electronic health record systems, interoperability, logging, and conformity assessment [6, 34, 35].

Germany's DiGA pathway connects access to reimbursement with requirements concerning evidence, data protection, and security. Listing by the Federal Institute for Drugs and Medical Devices under Section 139e of Social Code Book V should not be characterized as universal authorization for health applications. Its transferable policy lesson is to evaluate intended use, evidence, and information safeguards together [36].

A Macedonian operator must assess national requirements, including Article 84 where relevant, as well as any EU rules applicable to its activities in the European market. Local approval does not establish GDPR compliance, and European product conformity does not displace domestic processing obligations [1, 20]. Chinese market entry

additionally requires applicable domestic medical-device registration or filing; EU conformity does not replace that assessment [37]. As an illustrative example, a platform connecting Bulgarian, German, Macedonian, and Chinese institutions requires separate assessments of treatment exchange, research purposes, participant roles, provider access, and international transfer. A processing contract alone cannot resolve independent reuse by a provider for its own purposes. This is an analytical scenario, not an observed project [1, 25, 28, 31, 32].

3.8 Patient benefit and public health policy

Record access may help patients understand treatment, detect inaccuracies, and seek a second opinion. The systematic review by D'Costa, Kuhn, and Fritz also identifies ethical and practical concerns: access without explanation can cause anxiety, transfer unwanted responsibility to patients, or exacerbate inequalities. A legal entitlement should therefore be supported by understandable language, professional assistance, and nondigital channels [38].

Clinical evidence makes accuracy especially relevant. In a US survey, 4,830 of 22,889 respondents who read ambulatory notes reported a perceived mistake (21.1%). These were patient reports, not independently adjudicated errors or estimates for the four countries. Nevertheless, the findings support studying accessible correction procedures as a patient-safety intervention [39].

Biomedical collaboration also raises technical questions. Rieke et al. describe federated learning, where institutions collaborate in model development without pooling raw records centrally. Keeping source records local can reduce certain disclosure pathways, but does not automatically establish anonymity, eliminate security risks, or satisfy transfer and genetic-resource rules. For imaging or genomic projects, architecture, lawful access, validation, and clinical safety require separate assessment [1, 28, 32, 40].

Baines et al. associate willingness to share data with sensitivity, purpose, recipient identity, trust, control, and perceived benefit. Their review does not establish one universally optimal consent arrangement. It supports differentiation between treatment, public-interest research, and commercial purposes, with information appropriate to each context [41].

At population level, reliable and lawfully accessible data can support surveillance, service evaluation, technology assessment, and identification of inequalities. These are plausible mechanisms of public benefit, not outcomes measured in this study. Kalkman et al. identify social value, distribution of risks and benefits, respect for individuals and groups, and public trust as central dimensions of responsible sharing [42]. A policy implication is that success should not be measured only by data volume or the number of connected institutions.

There is a potential for dual exclusion: limited digital skills may reduce patients' control over records while also affecting representation in research datasets. Evaluation should therefore examine the distribution of access and benefits across age, socioeconomic, and geographic groups. This is an interpretive recommendation requiring local empirical assessment, rather than an established comparative result for the four countries [38, 42].

Maintaining fragmented procedures may reduce immediate transition costs but impede exchange and auditability. Broad centralized access can facilitate use while concentrating consequences of misuse or failure. The approach supported here combines common interoperability and accountability standards with role- and purpose-specific access. Costs include training, authorization management, logs, independent oversight, and responses to patient requests. Expected benefits include continuity, fewer information errors, and more reliable research. No net economic benefit or country ranking can be calculated from this documentary review [1, 6, 42].

3.9 Limitations

The analysis covers Germany's federal core and principal national instruments in Bulgaria, North Macedonia, and mainland China. It does not comprehensively examine state hospital legislation, specialized registries, or domestic case law. Institutional consolidated texts have different update dates; identified later amendments were examined separately. Retrieval does not constitute certified consolidation of every instrument at the cutoff. The Macedonian base law was examined through the agency's unofficial English translation alongside original amendments. Chinese sources included official English translations and Chinese texts; interpretive uncertainty and the evolving genetic-resources rules remain limitations.

Institutional reports reflect their own reporting periods. Legal analysis cannot establish actual cybersecurity performance or causal effects on health outcomes. The medical literature was selected purposively and is not restricted to the four jurisdictions; patient attitudes and implementation effects require local study. Product-market analysis addresses the relationship between data protection, EU product rules, and reimbursement, rather than a comprehensive review of every national licensing pathway.

4 CONCLUSION

Germany and Bulgaria share an EU foundation but implement health-information protection through different sectoral mechanisms. North Macedonia has adopted substantial European concepts while retaining distinctive approval rules and questions of coherence. China adds a distinct combination of sensitive-information safeguards, administrative supervision, and genetic-resource controls. Across the four systems, usable rights, effective oversight, and organizational implementation influence whether legal safeguards work in daily care. The EHDS makes the distinction between current obligations and future preparedness particularly important.

Practical recommendations follow from this comparison. First, organizations should document treatment, administration, research, and communication as distinct purposes, with corresponding grounds, recipients, and retention rules. This operationalizes accountability and reduces reliance on blanket consent [1, 20, 28]. Second, individual access permissions should follow professional need and be periodically reviewed, with auditable records. Recording reasons for emergency access and conducting subsequent review are proposed implementation practices consistent with preventive protection; they are not asserted to be identical express requirements in every jurisdiction [2, 8].

Third, organizations should assess the need for a data protection impact assessment before deployment and perform it where required. Macedonian Article 84 and Chinese PIPL Article 55 must be assessed on their own terms, separately from GDPR Article 36 prior consultation. Agency instruments can support analysis without replacing evaluation of actual risk [1, 20, 26, 28]. Fourth, patients should have understandable access, correction, and complaint procedures usable without a smartphone. Correction should preserve clinically necessary traceability of original entries [13, 24, 38].

Fifth, provider contracts should address actual roles, subcontractors, locations, remote access, incidents, and return or deletion of copies. International transfers require a separate assessment, including Chinese export and genetic-resource rules where applicable. Sixth, research access should be linked to defined purposes, minimized datasets, secure environments, and public information on results where legally required. Patient participation in governance is a complementary recommendation, with transparent conflict-of-interest arrangements [1, 6, 14, 25, 31, 32, 42].

National priorities differ: coordination of layered rules in Germany, coherent NHIS preparation for the EHDS in Bulgaria, alignment of transfer safeguards and supervisory capacity in North Macedonia, and coordination of patient rights, export controls, and biomedical governance in China. Evaluation could track response times to patient requests, review of permissions, completion of required risk assessments, incident response, and publication of research results. Low reported breach counts alone cannot establish security. Public value emerges when confidentiality, accuracy, and lawful availability jointly support patient autonomy, safe care, and accountable knowledge generation [12, 18, 23, 27].

ACKNOWLEDGEMENTS

OpenAI ChatGPT assisted with source retrieval, drafting, English translation, and manuscript formatting.

REFERENCES

[1] European Parliament, Council of the European Union. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. OJ L 2016;119:1–88. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng [accessed 2026 Sep 24].

[2] European Court of Human Rights. I. v. Finland. Application no. 20511/03. Judgment of 17 July 2008. Available from: https://hudoc.echr.coe.int/app/conversion/pdf/?filename=001-87510.pdf&id=001-87510&library=echr [accessed 2026 Sep 24].

[3] European Union. Charter of Fundamental Rights of the European Union. OJ C 2012;326:391–407. Articles 7, 8, 35, 51. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P008 [accessed 2026 Sep 24].

[4] Commission for Personal Data Protection. Circumstances in which consent to personal data processing is not required [in Bulgarian]. 2018 Jul 5. Available from: https://cpdp.bg/home-default/в-кои-случаи-не-се-изисква-съгласие-за-2/ [accessed 2026 Sep 24].

[5] Court of Justice of the European Union. FT v. DW. Case C-307/22. Judgment of 26 October 2023. ECLI:EU:C:2023:811. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0307 [accessed 2026 Sep 24].

[6] European Parliament, Council of the European Union. Regulation (EU) 2025/327 of 11 February 2025 on the European Health Data Space. OJ L 2025;2025/327. Available from: https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng [accessed 2026 Sep 24].

[7] European Commission. European Health Data Space Regulation (EHDS): implementation timeline [Internet]. Available from: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en [accessed 2026 Sep 24].

[8] Federal Republic of Germany. Bundesdatenschutzgesetz [Federal Data Protection Act]. 2017. Sections 22, 27 [in German; current online text]. Available from: https://www.gesetze-im-internet.de/bdsg_2018/ [accessed 2026 Sep 24].

[9] Federal Republic of Germany. Strafgesetzbuch [Criminal Code]. Section 203, Verletzung von Privatgeheimnissen [in German; current online text]. Available from: https://www.gesetze-im-internet.de/stgb/__203.html [accessed 2026 Sep 24].

[10] Federal Republic of Germany. Bürgerliches Gesetzbuch [Civil Code]. Section 630g, Einsichtnahme in die Behandlungsakte [in German; current online text]. Available from: https://www.gesetze-im-internet.de/bgb/__630g.html [accessed 2026 Sep 24].

[11] Federal Republic of Germany. Sozialgesetzbuch V [Social Code Book V]. Section 341, Elektronische Patientenakte [in German; current online text]. Available from: https://www.gesetze-im-internet.de/sgb_5/__341.html [accessed 2026 Sep 24].

[12] Federal Ministry of Health. Die ePA für alle [The electronic patient record for all] [Internet; in German]. Available from: https://www.bundesgesundheitsministerium.de/themen/digitalisierung/elektronische-patientenakte/epa-fuer-alle [accessed 2026 Sep 24].

[13] Federal Ministry of Health. FAQ zum Gesundheitsdatennutzungsgesetz [Questions and answers on the Health Data Use Act] [Internet; in German]. Available from: https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/gesundheitsdatennutzungsgesetz/faq-gesundheitsdatennutzungsgesetz [accessed 2026 Sep 24].

[14] Federal Republic of Germany. Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens [Health Data Use Act]. 2024. Sections 3–8 [in German]. Available from: https://www.gesetze-im-internet.de/gdng/ [accessed 2026 Sep 24].

[15] Republic of Bulgaria. Constitution of the Republic of Bulgaria. State Gazette 1991;56. Article 32 [official English version]. Available from: https://www.parliament.bg/en/const [accessed 2026 Sep 24].

[16] Republic of Bulgaria. Personal Data Protection Act. State Gazette 2002;1, as amended. Institutional text published by the supervisory commission [in Bulgarian]. Available from: https://cpdp.bg/правна-рамка-национална/закон-за-защита-на-личните-данни-2/ [accessed 2026 Sep 24].

[17] Republic of Bulgaria. Health Act. State Gazette 2004;70, as amended. Articles 27–28d, 86. Ministry of Health consolidated text dated 2024 Oct 14 [in Bulgarian]. Available from: https://www.mh.government.bg/upload/12273/Zakon%20za%20zdraveto%2014-10-2024.pdf [accessed 2026 Sep 24].

[18] Ministry of Health of Bulgaria. Ordinance No. N-6 of 21 December 2022 on the functioning of the National Health Information System. State Gazette 2022;103 [in Bulgarian]. Available from: https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=182160 [accessed 2026 Sep 24].

[19] Ministry of Health of Bulgaria. Ministerial response concerning continuity of the electronic health record after full adoption. Parliamentary control; 2026 [in Bulgarian]. Available from: https://mh.government.bg/bg/novini/parlamentaren-kontrol/4866 [accessed 2026 Sep 24].

[20] Republic of North Macedonia. Law on Personal Data Protection. Official Gazette 2020;42; amended by 2021;294 and 2025;101. Agency-published unofficial English translation of the base law. Available from: https://azlp.mk/wp-content/uploads/2022/12/lpdp_2020.pdf [accessed 2026 Sep 24].

[21] Republic of North Macedonia. Law amending and supplementing the Law on Personal Data Protection. Official Gazette 2021;294. 2021 Dec 27 [in Macedonian]. Available from: https://azlp.mk/wp-content/uploads/2022/11/57d665472d164493815e8b3bdcf8e2a1.pdf [accessed 2026 Sep 24].

[22] Republic of North Macedonia. Law supplementing the Law on Personal Data Protection. Official Gazette 2025;101. 2025 May 21 [in Macedonian]. Available from: https://azlp.mk/wp-content/uploads/2026/01/Zakon_za_dopolnuvanje_na_ZZLP-1.pdf [accessed 2026 Sep 24].

[23] European Commission. North Macedonia 2025 report. Commission staff working document. Brussels: European Commission; 2025 Nov 4. p. 36–7. Available from: https://enlargement.ec.europa.eu/document/download/267b368e-6b55-4a42-bb72-6395593de4da_en?filename=north-macedonia-report-2025.pdf [accessed 2026 Sep 24].

[24] Republic of North Macedonia. Law on the Protection of Patients' Rights. Official Gazette 2008;82; 2009;12; 2011;53; 2015;150. Editorial consolidated text, Articles 22–25; subsequent amendment 2019;190 [in Macedonian]. Available from: https://portal.mdt.gov.mk/post-body-files/zakoni-zdravstvo-file-t8E8.pdf [accessed 2026 Sep 24].

[25] European Commission. Adequacy decisions [Internet]. Available from: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [accessed 2026 Sep 24].

[26] Personal Data Protection Agency of North Macedonia. By-laws for the protection of personal data: security, impact assessment, and breach notification instruments. Official Gazette 2020;122 [Internet]. Available from: https://azlp.mk/en/pdpa/regulations-and-documents/by-laws-for-the-protection-of-personal-data/ [accessed 2026 Sep 24].

[27] Personal Data Protection Agency of North Macedonia. Strategy for implementing the right to personal data protection 2025–2030. 2024 [in Macedonian]. Available from: https://azlp.mk/wp-content/uploads/2024/11/Strategija_2025-2030_mk.pdf [accessed 2026 Sep 24].

[28] National People's Congress. Personal Information Protection Law of the People's Republic of China. 2021 Aug 20; effective 2021 Nov 1. Official English translation, paginated. Available from: https://en.spp.gov.cn/2021-12/29/c_948419.htm [accessed 2026 Sep 24].

[29] National People's Congress. Civil Code of the People's Republic of China. 2020 May 28. Articles 1225–1226 [in Chinese]. Available from: https://fgk.chinatax.gov.cn/zcfgk/c100009/c5212250/content.html [accessed 2026 Sep 24].

[30] State Council of the People's Republic of China. Network Data Security Management Regulations. Order No. 790. 2024 Sep 24; effective 2025 Jan 1 [in Chinese]. Available from: https://www.cac.gov.cn/2024-09/30/c_1729384452307680.htm [accessed 2026 Sep 24].

[31] Cyberspace Administration of China. Provisions on Promoting and Regulating Cross-border Data Flows. Order No. 16. 2024 Mar 22 [in Chinese]. Available from: https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm [accessed 2026 Sep 24].

[32] State Council of the People's Republic of China. Regulations on the Administration of Human Genetic Resources. 2019; amended 2024. Official health-bureau republication [in Chinese]. Available from: https://wjw.wuxi.gov.cn/doc/2024/06/04/4323063.shtml [accessed 2026 Sep 24].

[33] National Health Commission of China. Public consultation on draft implementing rules for the Regulations on the Administration of Human Genetic Resources. 2026 May 8 [in Chinese; consultation draft]. Available from: https://www.nhc.gov.cn/wjw/yjzj/202605/9b38dffa8d8047ea94813f40aca8d282.shtml [accessed 2026 Sep 24].

[34] European Parliament, Council of the European Union. Regulation (EU) 2017/745 of 5 April 2017 on medical devices. OJ L 2017;117:1–175. Available from: https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng [accessed 2026 Sep 24].

[35] European Commission. Certification of EHR systems [Internet]. Available from: https://health.ec.europa.eu/ehealth-digital-health-and-care/certification-ehr-systems_en [accessed 2026 Sep 24].

[36] Federal Institute for Drugs and Medical Devices. The fast-track process for digital health applications (DiGA) according to Section 139e SGB V: guide [Internet]. Available from: https://www.bfarm.de/SharedDocs/Downloads/EN/MedicalDevices/DiGA_Guide.pdf?__blob=publicationFile [accessed 2026 Sep 24].

[37] National Medical Products Administration. Announcement on implementation of the provisions for medical device registration and filing and in-vitro diagnostic reagent registration and filing. 2021 Sep 29 [Internet]. Available from: https://english.nmpa.gov.cn/2021-09/29/c_693367.htm [accessed 2026 Sep 24].

[38] D'Costa SN, Kuhn IL, Fritz Z. A systematic review of patient access to medical records in the acute setting: practicalities, perspectives and ethical consequences. BMC Med Ethics 2020;21:18. https://doi.org/10.1186/s12910-020-0459-6.

[39] Bell SK, Delbanco T, Elmore JG, et al. Frequency and types of patient-reported errors in electronic health record ambulatory care notes. JAMA Netw Open 2020;3(6):e205867. https://doi.org/10.1001/jamanetworkopen.2020.5867.

[40] Rieke N, Hancox J, Li W, et al. The future of digital health with federated learning. NPJ Digit Med 2020;3:119. https://doi.org/10.1038/s41746-020-00323-1.

[41] Baines R, Stevens S, Austin D, et al. Patient and public willingness to share personal health data for third-party or secondary uses: systematic review. J Med Internet Res 2024;26:e50421. https://doi.org/10.2196/50421.

[42] Kalkman S, Mostert M, Gerlinger C, et al. Responsible data sharing in international health research: a systematic review of principles and norms. BMC Med Ethics 2019;20:21. https://doi.org/10.1186/s12910-019-0359-9.