Digital Health Records and Informed Consent: Legal Challenges in The Adoption of Electronic Medical Systems

AUGUSTINE ONYEKA OKOLI[1], IRENE SAGAY[2], SANDRA OPARAH[3], OPEOLUWA OLUWANIFEMI AJAYI[4], COLLINS NWANNEBUIKE NWOKEDI[5]
[1]*Longmed Medical Centre, Pietermaritzburg, South Africa*
[2]*Independent Researcher, MD, USA*
[3]*Indepentent Researcher, MD, USA*
[4]*Amazing Grace Adult Home, Akure Ondo State*
[5]*Umgeni Psychiatric Hospital Medical, Pietermaritzburg, South Africa*

Abstract- ***The rapid adoption of Electronic Medical Systems (EMS) and Digital Health Records (DHR) has significantly transformed healthcare delivery, enhancing data accessibility, efficiency, and continuity of care. However, this digital shift has also introduced complex legal challenges, particularly regarding informed consent. Traditionally grounded in principles of patient autonomy and the right to self-determination, informed consent requires that patients fully understand the nature, purpose, and implications of their medical care. In the digital context, this obligation becomes more intricate due to the vast and often opaque processes surrounding data collection, storage, sharing, and automated decision-making. One of the primary legal concerns is the complexity and comprehensibility of digital consent mechanisms. Many consent forms presented within EMS platforms are overly technical, reducing patients' ability to make informed choices about data usage and sharing. Additionally, there is growing legal scrutiny of the validity of consent obtained through digital interfaces, especially where automated systems, artificial intelligence (AI), or algorithmic nudging influence decision-making processes. These technologies raise questions about the sufficiency of "informed" consent and whether patients can meaningfully control their health information. Data privacy and cybersecurity risks further complicate informed consent. Cross-border data transfers, cloud storage, and third-party integrations heighten exposure to breaches and unauthorized access, challenging compliance with stringent data protection laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Jurisdictional variations in legal recognition of electronic consent and differing cybersecurity standards create additional compliance complexities for healthcare providers. This highlights the urgent need for legal reforms and patient-centered technological designs to ensure that informed consent remains effective and meaningful in digital healthcare environments. It underscores the necessity of harmonized legal frameworks, robust cybersecurity measures, and accessible, transparent consent processes to uphold patient rights in the era of digital health records and electronic medical systems.***

Indexed Terms- ***Digital Health Records, Informed Consent, Legal Challenges, Adoption, Electronic Medical Systems***

I. INTRODUCTION

The rapid advancement of digital technologies has profoundly transformed healthcare delivery worldwide (Ogungbenle and Omowole, 2012; Mustapha *et al*., 2018). Central to this transformation is the widespread adoption of Electronic Medical Systems (EMS) and Digital Health Records (DHR), which serve as foundational tools for storing, processing, and sharing patient health information. Electronic Medical Systems (EMS) refer to

integrated software platforms that enable healthcare providers to manage clinical workflows, including patient registration, diagnostics, treatment plans, and billing (Syzdykova *et al*., 2017; Martin *et al*., 2018). Within these systems, Digital Health Records (DHR)—also commonly known as Electronic Medical Records (EMRs) or Electronic Health Records (EHRs)—are structured, digital versions of patients' medical histories, encompassing clinical notes, laboratory results, imaging data, medication lists, and other relevant health information (Norris and Bain, 2016; Azizi *et al*., 2016).

These technologies offer numerous benefits, including improved efficiency, enhanced coordination of care, and greater accessibility of patient information across healthcare settings (Dixon *et al*., 2018; Aceto *et al*., 2018). EMS and DHR facilitate evidence-based clinical decision-making, reduce medical errors, and support population health management by enabling large-scale data analytics. In many countries, digital health records are also integral to national health strategies aimed at achieving universal health coverage and improving healthcare quality (Asi and Williams, 2018; Konduri *et al*., 2018). Governments, health systems, and private entities are investing heavily in digital health infrastructure, with accelerated adoption during the COVID-19 pandemic further highlighting the potential of EMS and DHR to strengthen healthcare resilience.

Despite these advantages, the growing global reliance on digital health technologies raises critical ethical, legal, and regulatory concerns—foremost among them being informed consent (Vayena *et al*., 2018; Bruynseels *et al*., 2018). Informed consent is a cornerstone of medical ethics and human rights law, grounded in the principles of patient autonomy, self-determination, and bodily integrity. It requires healthcare providers to disclose relevant information about medical interventions, including associated risks, benefits, and alternatives, enabling patients to make voluntary, informed decisions regarding their care. In traditional healthcare settings, informed consent typically involves face-to-face communication between providers and patients (Tates *et al*., 2017; Atherton *et al*., 2018). However, in digital health environments, obtaining meaningful consent has become increasingly complex.

The digitization of health records introduces novel challenges to informed consent, particularly in relation to data privacy, security, and secondary uses of health data (Tresp *et al*., 2016; McLoughlin *et al*., 2017). Patients may be unaware of the full extent of how their personal health information is collected, stored, shared, and analyzed within EMS platforms. Consent processes embedded within digital systems are often presented as standard, non-negotiable terms, reducing patient agency. Moreover, automated data processing, cloud storage, and cross-border data transfers further complicate patients' understanding and control over their digital health information (Reichel, 2017; Conley and Pocs, 2018).

Additionally, emerging technologies such as artificial intelligence (AI)-driven decision support systems, predictive analytics, and remote monitoring devices rely on large volumes of personal health data, necessitating new models of informed consent. These developments raise questions about how consent can be meaningfully obtained in digital contexts, whether traditional legal frameworks sufficiently address evolving risks, and how to balance innovation with individual rights (Vayena and Gasser, 2016; Grundmann and Hacker, 2017).

Against this backdrop, the purpose of this review is to critically examine the legal challenges surrounding informed consent in the context of Electronic Medical Records (EMRs) and broader digital health systems. This explores the tension between the operational demands of digital health technologies and the ethical-legal imperatives of safeguarding patient autonomy and privacy. By analyzing key case law, regulatory frameworks, and international human rights standards, this seeks to illuminate gaps and ambiguities in existing consent practices and legal protections.

The study specifically focuses on issues such as the adequacy of digital consent mechanisms, the validity of blanket or broad consent for secondary data use, and the enforceability of patient rights within EMS platforms. The analysis spans multiple jurisdictions, including the European Union (under the General

Data Protection Regulation), the United States (under HIPAA and other federal statutes), and selected Global South countries, offering comparative insights into diverse regulatory approaches.

Ultimately, this aims to advance legal scholarship on informed consent in digital health, providing recommendations for more robust, transparent, and patient-centered consent frameworks that align with technological innovation while upholding ethical and legal standards in healthcare.

II. METHODOLOGY

The methodology for this study followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a transparent and rigorous review of the legal challenges related to digital health records and informed consent in the adoption of electronic medical systems. A comprehensive literature search was conducted across multiple academic databases, including PubMed, Scopus, Web of Science, HeinOnline, and Google Scholar, covering publications from January 2000 to 2018. The search combined keywords and subject headings such as "digital health records," "electronic medical records," "informed consent," "health data privacy," "data protection law," and "legal challenges in health informatics."

Eligibility criteria were predefined to include peer-reviewed journal articles, legal case analyses, regulatory reports, and policy papers that addressed the intersection of electronic medical records (EMRs), informed consent, and legal or ethical considerations. Studies focusing exclusively on technical or engineering aspects without legal analysis were excluded. Only publications in English were included.

After removing duplicate entries, titles and abstracts of retrieved records were screened independently by two reviewers to identify potentially relevant studies. Full-text screening followed for articles deemed relevant during the initial screening phase. Disagreements between reviewers were resolved through discussion or by consulting a third reviewer.

Data were extracted using a standardized form capturing study characteristics, jurisdictional focus, main legal issues discussed, ethical implications, and recommendations for law or policy reform. Specific attention was given to issues such as consent models for digital health data, data security obligations, interoperability challenges, liability risks, and patient autonomy concerns.

Quality assessment of the included studies was performed using adapted appraisal tools appropriate for legal and policy research, focusing on methodological rigor, clarity of argumentation, and relevance to the research question.

Findings were synthesized narratively, categorizing legal challenges under themes such as informed consent complexities, data protection and privacy law compliance, and liability in digital health ecosystems. This approach enabled a comparative analysis across jurisdictions, highlighting both common trends and context-specific legal frameworks in the regulation of electronic medical records and informed consent.

2.1 Legal Foundations of Informed Consent in Healthcare

The legal doctrine of informed consent has deep historical roots in both medical ethics and human rights law as shown in figure 1(Katz *et al*., 2016; Cocanour, 2017). Initially grounded in the Hippocratic tradition, where physicians were expected to act in patients' best interests, medical practice historically emphasized beneficence over patient autonomy. However, by the early 20th century, legal systems began shifting toward recognizing patients' rights to make their own medical decisions.

One of the earliest legal recognitions of consent occurred in Schloendorff v. Society of New York Hospital (1914), where Justice Benjamin Cardozo famously declared, "Every human being of adult years and sound mind has a right to determine what shall be done with his own body." This case laid the groundwork for modern informed consent by affirming bodily integrity and personal decision-making authority.

In the mid-20th century, the horrors of unethical medical experiments during World War II—most notably the Nazi experiments—prompted the formulation of the Nuremberg Code (1947), which established voluntary consent as an essential prerequisite for medical research. This was followed by the Declaration of Helsinki (1964), which reinforced ethical standards for medical research, particularly regarding the information provided to participants.

Figure 1: Key legal principles

In clinical care, the doctrine of informed consent further evolved through landmark court decisions in the United States and other common law jurisdictions. The emphasis shifted from merely obtaining consent to ensuring that patients received sufficient information to make informed decisions about their treatment (Bester *et al*., 2016; Nusbaum *et al*., 2017).

The core legal principles underpinning informed consent are autonomy, self-determination, and the duty of disclosure. These principles guide legal obligations imposed on healthcare providers and institutions.

Autonomy refers to the individual's right to control their own body and medical choices. It is a foundational value in both medical ethics and constitutional law, emphasizing the right of patients to accept or refuse medical interventions based on personal beliefs, values, and preferences.

Self-determination builds upon autonomy, stressing the patient's authority to make voluntary decisions free from coercion, manipulation, or undue influence (Thomas, 2017; Dive and Newson, 2018). Self-determination has been recognized as a fundamental human right under various international legal instruments, including the International Covenant on Civil and Political Rights (ICCPR).

The duty of disclosure requires healthcare providers to furnish patients with adequate, relevant information to make informed decisions. This includes details about the nature and purpose of proposed treatments, potential risks and benefits, available alternatives, and likely outcomes. The duty of disclosure is not merely a procedural requirement but a substantive obligation grounded in respect for patient dignity and legal rights.

Courts have generally held that the adequacy of disclosure depends on factors such as the patient's specific circumstances, the risks involved, and prevailing medical standards (Price and Nicholson, 2017; Parasidis, 2017). Two primary legal standards are often applied; Professional Standard, disclosure based on what a reasonable medical practitioner would provide. Reasonable Patient Standard, disclosure based on what a reasonable patient would find significant in making a decision.

Several landmark cases have shaped informed consent obligations worldwide.

In the United States, Canterbury v. Spence (1972) established the reasonable patient standard, holding that physicians must disclose information that an average patient would deem necessary to make an informed choice. This case shifted the focus from professional customs to patient-centered disclosure.

In the United Kingdom, Montgomery v. Lanarkshire Health Board (2015) similarly emphasized patient autonomy, ruling that doctors must take reasonable care to ensure that patients are aware of material risks and reasonable alternatives. The UK Supreme Court stressed that the medical paternalism traditionally accepted in British law must give way to respect for patient autonomy (Cave, 2017; Lloyd, 2018).

In Canada, cases such as Reibl v. Hughes (1980) and Hopp v. Lepp (1980) reinforced the importance of patient-centered disclosure, adopting a hybrid approach that incorporates both professional and reasonable patient standards.

In India, the Supreme Court has invoked constitutional rights to bodily integrity and privacy to strengthen informed consent protections, particularly in cases involving sterilization and reproductive rights, such as Suchita Srivastava v. Chandigarh Administration (2009).

These cases reflect a growing global consensus that informed consent is not merely a procedural formality but a fundamental legal and ethical obligation that healthcare providers must uphold (Pilegaard, 2016; Campbell and Parsi, 2017).

Various statutory and regulatory frameworks reinforce the legal foundations of informed consent in healthcare.

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) safeguards patients' rights to access their health information and requires informed consent for the disclosure of protected health information (PHI). While HIPAA focuses on data privacy, it intersects with informed consent in areas involving digital health records, telemedicine, and health data sharing (Ostherr *et al*., 2017; McSwain *et al*., 2017).

The General Data Protection Regulation (GDPR) of the European Union provides robust protections for personal data, including health data. GDPR's consent requirements emphasize that consent must be freely given, specific, informed, and unambiguous. It also grants individuals the right to withdraw consent at any time. While GDPR primarily addresses data protection, its principles significantly affect how healthcare providers obtain and manage consent for digital health records and health data processing.

In Australia, the Privacy Act 1988 and related health privacy regulations establish clear consent obligations regarding the collection, use, and disclosure of health information.

Many countries also have specific national health acts that codify informed consent obligations. For instance, South Africa's National Health Act (2003) explicitly requires healthcare providers to obtain informed consent before treatment, unless exceptions apply, such as emergencies where consent cannot be obtained.

International organizations such as the World Health Organization (WHO) and Council of Europe have also developed guidelines on informed consent, particularly regarding cross-border healthcare, research ethics, and digital health systems (Wicclair, 2016; Thorogood *et al*., 2018).

Informed consent is a legally and ethically indispensable component of modern healthcare, deeply rooted in historical developments, court decisions, and regulatory frameworks. It embodies fundamental principles of autonomy, self-determination, and disclosure, shaping legal duties for healthcare providers across jurisdictions. As healthcare increasingly digitizes, understanding these legal foundations is crucial to safeguarding patient rights and ensuring that informed consent remains meaningful in evolving technological and clinical environments (Mello *et al*., 2018; Blix and Levay, 2018).

2.2 Digital Health Records and Informed Consent: Conceptual Intersections

The digital transformation of healthcare has introduced significant shifts in the way medical data is managed, with Electronic Health Records (EHRs) replacing traditional paper-based systems in many healthcare settings (Sullivan *et al*., 2016; Scott *et al*., 2018). While this transition has improved the efficiency and accuracy of healthcare delivery, it has also introduced new legal, ethical, and operational complexities, particularly regarding informed consent. Understanding the conceptual intersections between digital health records and informed consent requires examining the distinctive characteristics of digital records, the evolving role of consent in data management, and the emergence of innovative digital consent models.

Digital health records possess several distinctive features that differentiate them from paper-based medical records. One of the most salient differences is their enhanced accessibility and interoperability. EHRs enable authorized healthcare providers to access patient data in real time across multiple locations, facilitating continuity of care and

improving clinical decision-making (Azaria *et al*., 2016; Saiod *et al*., 2017). This capacity for rapid information sharing, however, raises concerns about unauthorized access and data security. Unlike paper records, which are confined to physical spaces and inherently limited in distribution, digital records are vulnerable to cybersecurity threats, including hacking, ransomware attacks, and unauthorized third-party access.

Another distinctive feature is the scalability of digital records. EHRs can store vast quantities of diverse data types, including structured clinical information, diagnostic imaging, genomic data, and patient-generated health information from wearable devices. While this richness of data enhances the potential for precision medicine and advanced analytics, it also complicates consent processes, as patients may not fully understand the breadth and depth of data being collected or its potential uses.

Furthermore, digital health records enable automated data processing through artificial intelligence and machine learning algorithms. These technologies can analyze patterns within patient data to support clinical decision-making or predict health risks (Belard *et al*., 2017; Islam *et al*., 2018). However, automated processing introduces new questions about transparency and patient agency, particularly when patients are unaware that their data is being subjected to algorithmic analysis.

Within this context, the role of informed consent in data collection, storage, sharing, and access has become increasingly complex. In traditional healthcare settings, informed consent primarily concerned treatment decisions and the disclosure of medical risks. In the digital era, however, informed consent must also encompass the collection and processing of personal health information, the storage of such information in cloud-based systems, and the potential sharing of data with multiple stakeholders, including insurers, researchers, and technology providers.

Consent for data collection and storage must account for the technical nature of digital health systems. Patients must be informed about what categories of data will be collected, how the data will be stored, and the security measures in place to protect it (Tucker *et al*., 2016; Banerjee *et al*., 2018). Moreover, patients must be aware of the duration of data retention and any legal or institutional policies governing data deletion or archival.

Data sharing further complicates consent, as digital health systems often involve multiple actors across various jurisdictions. Patients may need to provide consent not only for the initial collection of data but also for its transfer between different healthcare providers, research institutions, and digital platforms (Spencer *et al*., 2016; Ohmann *et al*., 2017). This sharing can be either direct, such as sharing between hospitals, or indirect, through de-identified data repositories for secondary research use. The legal and ethical challenge lies in ensuring that patients retain meaningful control over their data in such interconnected environments.

In response to these challenges, emerging models of digital consent have been developed to promote more nuanced and patient-centered approaches. Dynamic consent is one such model, allowing patients to adjust their consent preferences over time as their circumstances change or as new data uses emerge. Dynamic consent platforms typically offer user-friendly digital interfaces where patients can view, modify, or withdraw their consent for specific purposes at any point, thus promoting ongoing engagement and autonomy (Kyriazakos *et al*., 2017; Politou *et al*., 2018).

Tiered consent represents another approach, whereby patients are offered varying levels of consent options. For instance, a patient may consent to the use of their data for their immediate clinical care but may opt out of secondary uses such as research or marketing. This model aims to strike a balance between enabling beneficial data sharing and respecting individual preferences regarding privacy and data use.

Granular consent mechanisms take this approach further by allowing patients to specify consent at a highly detailed level, down to specific data elements or types of uses. For example, a patient could consent to the use of their demographic information for research but restrict the sharing of their genetic data. Granular consent mechanisms are particularly

valuable in genomics and precision medicine, where different data categories carry varying degrees of sensitivity (Ashley, 2016; Jensen *et al*., 2017).

Collectively, these emerging consent models aim to address the complexity of digital health records by offering patients greater control and flexibility. However, their implementation poses significant technical, legal, and ethical challenges. Ensuring that these consent mechanisms are both functional and accessible to diverse populations requires careful system design, regulatory oversight, and sustained patient education efforts.

The transition from paper-based records to digital health systems has fundamentally transformed the landscape of informed consent. As healthcare increasingly relies on data-driven technologies, consent processes must evolve to address the complexities of digital data collection, storage, sharing, and automated analysis. Emerging models such as dynamic, tiered, and granular consent provide promising pathways toward more ethical and patient-centered data governance, but they also require careful legal and technological alignment to protect patient rights while enabling medical innovation (Sund and White, 2016; Genesis, 2018).

2.3 Key Legal Challenges in Digital Health Records and Informed Consent

The digitization of healthcare through Electronic Medical Records (EMRs) and broader digital health systems has introduced significant legal complexities surrounding informed consent. While these systems improve efficiency and access to medical data, they also raise questions about consent validity, data protection, and patient autonomy in the digital environment as shown in figure 2(Mostert *et al*, 2016; Rumbold and Pierscionek, 2017). Three core legal challenges emerge: ensuring comprehensible consent, addressing data privacy risks, and resolving uncertainties in consent processes involving automation and artificial intelligence (AI).

One of the primary legal concerns in digital health systems is ensuring that consent mechanisms are truly understandable to patients. Informed consent is only valid when patients receive adequate, clear, and comprehensible information about the collection, use, and sharing of their health data (Bester *et al*., 2016; Kadam, 2017). In digital platforms, consent is often obtained via electronic forms, pop-up agreements, or app interfaces. However, these mechanisms frequently rely on dense, legalistic language that exceeds the average patient's reading ability.

Regulatory frameworks such as the EU's General Data Protection Regulation (GDPR) mandate that information provided in consent forms must be "concise, transparent, intelligible, and easily accessible." Similarly, the U.S. Health Information Technology for Economic and Clinical Health Act (HITECH Act) promotes clear patient communications in digital contexts. Nonetheless, many digital consent forms remain challenging for patients to comprehend, undermining the core purpose of informed consent.

Excessively technical language in digital consent forms can invalidate consent under legal standards that emphasize voluntariness and comprehension. Studies reveal that many digital health consent forms contain complex language, often at college reading levels, which poses a significant barrier for users with limited health literacy or non-native speakers. This issue is compounded in global digital health systems, where standardized consent forms may not align with cultural or linguistic norms.

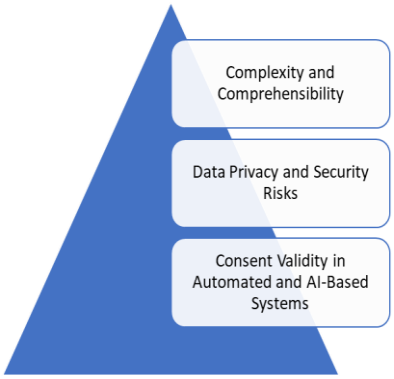

Figure 2: Key Legal Challenges in Digital Health Records and Informed Consent

Furthermore, digital systems often employ "click-wrap" or "browse-wrap" agreements, where consent is presumed upon accessing a service or clicking a button, with minimal patient engagement. These forms of consent are frequently criticized for failing

to meet the threshold of informed consent, as they obscure risks related to data sharing, third-party access, or secondary uses of health data (Sawicki, 2016; Kahn *et al*., 2018).

Several case studies highlight the gaps in digital informed consent. For instance, investigations into widely used COVID-19 contact tracing apps revealed significant shortcomings in user comprehension and consent transparency. In some jurisdictions, apps were deployed with minimal disclosure about data retention policies or third-party sharing, prompting legal challenges under GDPR and domestic privacy laws.

Similarly, in the United States, concerns were raised over mobile health apps that shared sensitive reproductive health data without adequate patient consent, leading to Federal Trade Commission (FTC) investigations. These cases underscore the need for enhanced legal standards and regulatory enforcement to ensure that digital consent is both accessible and meaningful.

Digital health systems are prime targets for cyberattacks and data breaches, given the sensitivity and value of health information. Legal liability for unauthorized access to EMRs presents significant challenges for healthcare providers and technology vendors alike. Courts and regulators must assess whether sufficient security measures were in place and whether patients were adequately informed about data risks.

Under GDPR, data controllers face strict liability for breaches involving insufficient consent or inadequate data protection measures (Gruschka *et al*., 2018; Keller, 2018). In the U.S., HIPAA imposes similar obligations, with breach notification requirements and potential financial penalties for negligent data handling. However, patients rarely have practical recourse for damages in many jurisdictions, especially in cases involving systemic vulnerabilities or third-party hacking.

Consent under privacy laws must satisfy specific criteria to be legally valid. GDPR, in particular, requires that consent be "informed, specific, unambiguous, and freely given," raising the bar for digital health platforms. Consent forms must clearly identify the data being collected, its purpose, and any third-party sharing arrangements.

However, legal tensions arise between privacy law consent and medical informed consent. While privacy laws focus on data use, medical informed consent typically concerns treatment risks and benefits. In digital health, these two consent regimes intersect, yet they are often treated separately, leading to fragmented protections and patient confusion.

Cross-border data transfers further complicate informed consent in digital health. Many cloud-based EMR systems involve storing patient data on servers located in different countries, raising jurisdictional issues about applicable privacy protections. Patients may not fully understand that their health data is subject to foreign laws, potentially undermining their control over personal information.

Legal mechanisms such as Standard Contractual Clauses (SCCs) under GDPR or the U.S. Privacy Shield Framework (which was invalidated in 2020) attempt to regulate international transfers, but these mechanisms are largely invisible to patients. The lack of transparency around cross-border data flows makes it difficult to obtain truly informed consent in global digital health systems.

Automated systems, including health chatbots, wearable devices, and patient portals, increasingly collect health data and obtain consent through algorithm-driven interfaces. However, there is significant legal uncertainty regarding the validity of such consent. Many automated platforms use pre-set defaults or "nudging" techniques to encourage consent, raising questions about voluntariness and undue influence.

Furthermore, legal systems differ in their recognition of consent obtained through automated systems. While some jurisdictions accept electronic consent under specific conditions, others maintain stricter requirements for explicit, human-mediated consent for sensitive health data.

"Algorithmic nudging," where users are subtly steered toward particular choices through design

features, poses a serious ethical and legal challenge in digital consent. Health apps may prioritize ease of use over privacy by presenting consent options in ways that favor data sharing (Moon, 2017; Househ *et al*., 2018). Such practices can undermine the voluntariness of consent and may be deemed coercive or manipulative.

Legal scholars and courts are increasingly scrutinizing these design strategies. GDPR's prohibition against "dark patterns" in consent mechanisms reflects this concern, but enforcement remains inconsistent, particularly in non-EU jurisdictions.

Finally, there is considerable variation across jurisdictions regarding the recognition of electronic signatures and digital consent. Some countries, such as the United States, broadly recognize electronic consent under laws like the Electronic Signatures in Global and National Commerce Act (ESIGN Act). Others, particularly in parts of Asia and Africa, impose stricter conditions or require in-person verification for sensitive health transactions.

These inconsistencies create legal uncertainty for multinational digital health providers, complicating efforts to harmonize consent processes across borders. They also pose risks to patients who may not fully understand the legal status of their digital consent.

Digital health records and technologies offer substantial benefits but also pose significant legal challenges for informed consent. Issues of comprehensibility, data privacy, and consent validity in automated environments raise complex questions about patient autonomy, legal compliance, and ethical practice. Addressing these challenges requires updated legal frameworks, enhanced regulatory oversight, and design strategies that prioritize transparency, simplicity, and respect for patient rights in the digital era (Leenes *et al*., 2017; Roth *et al*., 2018).

2.4 Jurisdictional Comparisons and Emerging Legal Trends

The regulation of informed consent in digital health varies significantly across jurisdictions, reflecting distinct legal traditions, privacy cultures, and technological landscapes (Mendelson, 2017; Kulynych and Greely, 2017). This provides a comparative analysis of major regulatory approaches in the United States, the European Union, and key Asia-Pacific jurisdictions, alongside emerging trends toward harmonization and the role of regional digital health networks in shaping consent frameworks.

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) forms the cornerstone of health data protection, with its Privacy Rule governing the use and disclosure of protected health information (PHI). HIPAA requires "authorization" for uses beyond treatment, payment, or healthcare operations, which effectively serves as a form of informed consent for data-sharing purposes. Authorizations must be specific, time-limited, and explicitly describe the data use purpose.

However, HIPAA has notable limitations. It applies only to "covered entities," such as healthcare providers, insurers, and their business associates, leaving gaps in digital health apps, wearable devices, and direct-to-consumer platforms that fall outside its regulatory scope. This fragmentation has prompted several U.S. states to enact more stringent laws. For example, California's Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) extend data protection obligations to a broader range of entities, including health-related apps not covered by HIPAA. These laws grant consumers explicit rights to access, delete, and opt out of data sales, thus supplementing federal protections.

State-level laws also introduce varying consent standards for digital health tools, complicating compliance for multi-state providers. Overall, the U.S. framework remains highly sectoral and decentralized, with growing calls for a comprehensive federal privacy law that integrates stronger consent requirements for digital health ecosystems.

The European Union leads globally in setting robust and unified data protection standards through the General Data Protection Regulation (GDPR). GDPR applies to all entities processing personal data within the EU, including digital health platforms. It

categorizes health data as "special category data," requiring heightened safeguards and explicit, informed consent for most processing activities unless a legal exemption applies (e.g., vital interests or public health purposes).

GDPR emphasizes that consent must be "freely given, specific, informed, and unambiguous," with additional requirements for data portability and the right to withdraw consent at any time. Digital health systems must ensure that patients understand the specific purposes for which their data will be used, particularly for secondary uses like research or AI-based analytics (Murray *et al*., 2016; Sundaravadivel *et al*., 2017).

In addition to GDPR, the ePrivacy Directive—commonly known as the "Cookie Law"—regulates electronic communications and imposes consent obligations for tracking technologies, which are increasingly relevant for digital health apps and telemedicine services. Together, these frameworks provide comprehensive protections but also impose complex compliance obligations, particularly for cross-border health platforms serving EU patients.

GDPR has catalyzed a shift toward privacy-by-design in digital health, requiring developers to integrate privacy and consent considerations throughout product lifecycles. Moreover, GDPR's extraterritorial reach influences non-EU jurisdictions, making it a de facto global standard for digital health consent in many cases.

Asia-Pacific jurisdictions exhibit growing regulatory sophistication in digital health consent, though approaches remain varied.

In India, the Digital Information Security in Healthcare Act (DISHA), still pending enactment, aims to establish comprehensive consent-based standards for electronic health data. DISHA proposes stringent consent requirements for the collection, storage, and exchange of personal health records, with an emphasis on explicit and informed consent for secondary data use. It also seeks to empower patients with rights to access and correct their digital health data. While DISHA's passage has been delayed, its principles have influenced ongoing debates on digital health governance in India.

Japan's Act on the Protection of Personal Information (APPI) governs personal data, including health information, and was significantly amended in 2020 to strengthen consent obligations. Under APPI, explicit consent is generally required for processing sensitive personal data, including for marketing or secondary research purposes. The amendments also introduced stricter rules for cross-border data transfers, mandating greater transparency and the right to request disclosure of data handling practices.

Both India and Japan illustrate the trend toward incorporating consent-based frameworks in digital health governance, though India's model is more centralized and healthcare-specific, while Japan's approach remains rooted in general privacy law (Burri, 2016; Edwards, 2016).

The growing complexity of cross-border digital health services has accelerated discussions around harmonizing consent frameworks. International bodies such as the Organisation for Economic Co-operation and Development (OECD) and the World Health Organization (WHO) have advocated for baseline global standards on digital health consent to address fragmentation and ensure equitable protections.

Key areas of emerging consensus include; The need for explicit and informed consent for sensitive health data processing. Requirements for clear, accessible consent language suited to diverse literacy levels. Patient rights to withdraw consent and to access, correct, or delete their data. Protections against algorithmic bias and discriminatory data use.

Although full global harmonization remains distant due to legal, cultural, and economic differences, regional models such as GDPR increasingly serve as templates for emerging laws in other jurisdictions, including parts of Asia, Africa, and Latin America.
Regional digital health collaborations also play a growing role in shaping consent policies. Initiatives like the European Health Data Space (EHDS) seek to create interoperable digital health infrastructures

across EU member states, anchored in robust consent management and patient control mechanisms.

Similarly, the ASEAN Digital Health Ecosystem has identified data governance and consent as priority areas for regional cooperation, with efforts underway to align national frameworks and facilitate secure cross-border data flows among Southeast Asian nations.

In Africa, the Smart Africa Digital Health Initiative promotes regional collaboration on digital health strategies, including harmonized consent protocols to support mobile health (mHealth) and telemedicine applications across borders.

These regional initiatives aim to strike a balance between facilitating digital health innovation and safeguarding patient autonomy, with shared standards for digital consent emerging as a critical enabler of cross-border health data interoperability.

The comparative analysis reveals significant divergences in legal approaches to digital health consent across the U.S., EU, and Asia-Pacific jurisdictions. However, emerging trends toward harmonization—driven by global privacy norms, technological interoperability, and regional health networks—suggest a gradual convergence on core principles of informed, transparent, and patient-centered consent. Future developments will likely require further legal innovation to bridge gaps between jurisdictions while respecting local contexts and healthcare priorities (Gottlieb *et al*., 2016; Finck, 2018).

2.5 Recommendations for Legal Reform and Best Practices

The digitalization of healthcare through Electronic Health Records (EHRs) has enhanced the efficiency and quality of care, but it has also exposed complex legal, ethical, and technical challenges related to informed consent. As digital health technologies expand, legal frameworks and best practices must evolve to safeguard patient autonomy, privacy, and data security. Effective legal reform and operational strategies should focus on creating user-centered consent systems, regulatory transparency, interoperability, cybersecurity, and professional education as shown in figure 3.

Figure 3: Recommendations for Legal Reform and Best Practices

A central recommendation for legal reform is the development of user-centric, accessible digital consent systems that empower patients to make informed decisions regarding their health data. Traditional consent forms, often lengthy and laden with technical jargon, are inadequate in digital contexts where rapid, remote data collection is common. Digital consent systems should be designed using plain, comprehensible language, supported by visual aids, interactive tools, or multilingual options to accommodate diverse patient populations. These systems should prioritize usability, allowing patients to easily review, understand, and adjust their consent preferences through intuitive interfaces. This may include dashboards where individuals can view data-sharing agreements, track data access history, and modify consent in real-time. Such design principles align with human-centered legal technology approaches, emphasizing transparency, control, and informed participation.

In tandem with usability improvements, clear regulatory guidelines are essential to ensure that consent processes on digital platforms are transparent, fair, and legally robust. Current regulations, such as the European Union's General Data Protection Regulation (GDPR), require consent to be specific, informed, and freely given, yet many healthcare platforms fall short of meeting these standards in practice. National and regional legislatures should establish standardized digital consent protocols for healthcare, specifying

requirements for consent clarity, revocability, and informed choice. These guidelines should explicitly define what constitutes valid digital consent, clarify the legal status of digital signatures, and ensure that consent withdrawal is as easy as its provision. Additionally, regulators should mandate periodic audits and compliance reporting for digital consent processes, ensuring ongoing adherence to legal and ethical obligations.

Another critical area for legal and operational reform is the promotion of interoperability while maintaining strong patient control over data. Interoperability allows for seamless data exchange among healthcare providers, insurers, and researchers, which is essential for coordinated care and medical innovation. However, without appropriate safeguards, interoperability can undermine privacy and erode patient trust. Legal reforms should require that interoperability frameworks integrate consent management functionalities, enabling patients to specify consent at granular levels for different data uses and across various systems. Health information exchange networks must ensure that patient preferences are communicated consistently throughout the data-sharing chain. Furthermore, policymakers should consider adopting open technical standards for consent management APIs, ensuring that digital health platforms can interoperate without compromising patient consent rights.

Mandatory cybersecurity safeguards tied to informed consent obligations are equally critical in digital healthcare ecosystems. Given the heightened risk of cyberattacks targeting healthcare systems, regulatory reforms must establish minimum security standards for any entity handling digital health data. Encryption, multi-factor authentication, regular vulnerability testing, and incident response protocols should be legally required, with clear accountability for data breaches. Importantly, informed consent processes must explicitly disclose potential cybersecurity risks to patients, detailing how their data is protected and what recourse is available in the event of a breach. Regulators may also mandate third-party cybersecurity certifications for digital health vendors to assure compliance with industry best practices.

Finally, effective reform requires investment in training healthcare professionals on digital consent laws, ethical data stewardship, and patient-centered communication. Many healthcare providers are unfamiliar with the legal complexities of digital consent and may inadvertently engage in non-compliant practices. Comprehensive training programs should be embedded into medical education and continuing professional development, focusing on the legal foundations of digital consent, the ethical use of patient data, and practical skills in utilizing digital consent tools. Interdisciplinary education, involving legal experts, ethicists, and technologists, can prepare healthcare workers to navigate evolving digital health landscapes responsibly. In addition, healthcare organizations should appoint specialized data protection officers or digital consent advisors to support frontline staff in complex consent scenarios.

The evolution of digital health technologies necessitates a rethinking of informed consent practices through both legal reform and institutional best practices. Designing user-centric consent interfaces, establishing robust regulatory frameworks, enhancing interoperability with patient control, mandating cybersecurity safeguards, and educating healthcare professionals are all essential strategies for building trustworthy, transparent, and ethical digital healthcare systems. By advancing these recommendations, policymakers and healthcare institutions can safeguard patient autonomy while fostering innovation and efficiency in modern healthcare delivery.

CONCLUSION

The rapid integration of digital health records and electronic medical systems has fundamentally reshaped healthcare delivery, making informed consent more complex and critically important. As health data is increasingly digitized, shared, and analyzed across platforms and borders, ensuring meaningful and legally valid informed consent has become a central challenge for health systems, regulators, and technology developers. This issue is not merely procedural; it directly affects patient autonomy, privacy, and trust in healthcare institutions. Without robust consent mechanisms,

digital health risks undermining core ethical and legal principles that protect individual rights.

Balancing technological innovation with patient rights and legal protections remains a delicate task. On the one hand, digital health tools—such as electronic health records, telemedicine platforms, and AI-powered decision-support systems—offer immense potential to improve healthcare quality, efficiency, and accessibility. On the other hand, these technologies can expose patients to new risks of data misuse, surveillance, and loss of control over personal information. Current legal frameworks often struggle to keep pace with rapidly evolving technologies, leading to gaps in protection, especially in automated or cross-border data environments. A nuanced, patient-centered approach is essential—one that integrates informed consent as a core design feature of digital health technologies, not just as a regulatory checkbox.

To address these challenges, there is an urgent need for multidisciplinary collaboration among legal experts, ethicists, healthcare providers, technologists, and patient advocates. Strengthening legal frameworks alone is insufficient without corresponding innovations in technology design that make consent processes transparent, accessible, and comprehensible. Co-designing consent systems with diverse stakeholders will help align legal compliance with patient empowerment and health equity. By embedding informed consent into both technological infrastructures and regulatory architectures, healthcare systems can foster trust, protect rights, and ensure that digital health innovations serve the public good.

REFERENCES

[1] Aceto, G., Persico, V. and Pescapé, A., 2018. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. *Journal of Network and Computer Applications*, *107*, pp.125-154.

[2] Ashley, E.A., 2016. Towards precision medicine. *Nature Reviews Genetics*, *17*(9), pp.507-522.

[3] Asi, Y.M. and Williams, C., 2018. The role of digital health in making progress toward Sustainable Development Goal (SDG) 3 in conflict-affected populations. *International journal of medical informatics*, *114*, pp.114-120.

[4] Atherton, H., Brant, H., Ziebland, S., Bikker, A., Campbell, J., Gibson, A., McKinstry, B., Porqueddu, T. and Salisbury, C., 2018. The potential of alternatives to face-to-face consultation in general practice, and the impact on different patient groups: a mixed-methods case study. *Health Services and Delivery Research*, *6*(20).

[5] Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A., 2016, August. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd international conference on open and big data (OBD)* (pp. 25-30). IEEE.

[6] Azizi, A., Aboutorabi, R., Mazloum-Khorasani, Z., Hoseini, B. and Tara, M., 2016. Diabetic personal health record: a systematic review article. *Iranian journal of public health*, *45*(11), p.1388.

[7] Banerjee, S., Hemphill, T. and Longstreet, P., 2018. Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, *34*(1), pp.49-57.

[8] Belard, A., Buchman, T., Forsberg, J., Potter, B.K., Dente, C.J., Kirk, A. and Elster, E., 2017. Precision diagnosis: a view of the clinical decision support systems (CDSS) landscape through the lens of critical care. *Journal of clinical monitoring and computing*, *31*, pp.261-271.

[9] Bester, J., Cole, C.M. and Kodish, E., 2016. The limits of informed consent for an overwhelmed patient: clinicians' role in protecting patients and preventing overwhelm. *AMA journal of ethics*, *18*(9), pp.869-886.

[10] Bester, J., Cole, C.M. and Kodish, E., 2016. The limits of informed consent for an overwhelmed patient: clinicians' role in protecting patients and preventing overwhelm. *AMA journal of ethics*, *18*(9), pp.869-886.

[11] Blix, M. and Levay, C., 2018. Digitalization and health care. *Eso expertgrupp*, *44*, pp.13-35.

[12] Bruynseels, K., Santoni de Sio, F. and Van den Hoven, J., 2018. Digital twins in health care: ethical implications of an emerging engineering paradigm. *Frontiers in genetics*, *9*, p.31.

[13] Burri, M., 2016. The regulation of data flows through trade agreements. *Geo. J. Int'l L.*, *48*, p.407.

[14] Campbell, K. and Parsi, K., 2017. A new age of patient transparency: an organizational framework for informed consent. *The Journal of Law, Medicine & Ethics*, *45*(1), pp.60-65.

[15] Cave, E., 2017. Protecting patients from their bad decisions: rebalancing rights, relationships, and risk. *Medical law review*, *25*(4), pp.527-553.

[16] Cocanour, C.S., 2017. Informed consent—It's more than a signature on a piece of paper. *The American Journal of Surgery*, *214*(6), pp.993-997.

[17] Conley, E. and Pocs, M., 2018. GDPR compliance challenges for interoperable health information exchanges (HIEs) and trustworthy research environments (TREs). *Eur. J. Biomed. Inform*, *14*, pp.48-61.

[18] Dive, L. and Newson, A.J., 2018. Reconceptualizing autonomy for bioethics. *Kennedy Institute of Ethics Journal*, *28*(2), pp.171-203.

[19] Dixon, B.E., Embi, P.J. and Haggstrom, D.A., 2018. Information technologies that facilitate care coordination: provider and patient perspectives. *Translational behavioral medicine*, *8*(3), pp.522-525.

[20] Edwards, L., 2016. Privacy, security and data protection in smart cities: A critical EU law perspective. *Eur. Data Prot. L. Rev.*, *2*, p.28.

[21] Finck, M., 2018. Blockchains: Regulating the unknown. *German Law Journal*, *19*(4), pp.665-692.

[22] Genesis, I.O., 2018. Integrative pharmacoeconomics: redefining pharmacists' role in formulary design and value-based healthcare systems. *Int J Comput Appl Technol Res*, *7*(12), pp.435-48.

[23] Gottlieb, L., Glymour, M.M., Kersten, E., Taing, E., Hagan, E., Vlahov, D. and Adler, N.E., 2016. Challenges to an integrated population health research agenda: Targets, scale, tradeoffs and timing. *Social Science & Medicine*, *150*, pp.279-285.

[24] Grundmann, S. and Hacker, P., 2017. Digital technology as a challenge to European contract law: from the existing to the future architecture. *European Review of Contract Law*, *13*(3), pp.255-293.

[25] Gruschka, N., Mavroeidis, V., Vishi, K. and Jensen, M., 2018, December. Privacy issues and data protection in big data: a case study analysis under GDPR. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 5027-5033). IEEE.

[26] Househ, M., Grainger, R., Petersen, C., Bamidis, P. and Merolli, M., 2018. Balancing between privacy and patient needs for health information in the age of participatory health and social media: a scoping review. *Yearbook of medical informatics*, *27*(01), pp.029-036.

[27] Islam, M.S., Hasan, M.M., Wang, X., Germack, H.D. and Noor-E-Alam, M., 2018, May. A systematic review on healthcare analytics: application and theoretical perspective of data mining. In *Healthcare* (Vol. 6, No. 2, p. 54). MDPI.

[28] Jensen, M.A., Ferretti, V., Grossman, R.L. and Staudt, L.M., 2017. The NCI Genomic Data Commons as an engine for precision medicine. *Blood, The Journal of the American Society of Hematology*, *130*(4), pp.453-459.

[29] Kadam, R.A., 2017. Informed consent process: a step further towards making it meaningful!. *Perspectives in clinical research*, *8*(3), pp.107-112.

[30] Kahn, J.P., Mastroianni, A.C. and Sugarman, J. eds., 2018. *Beyond consent: Seeking justice in research*. Oxford University Press.

[31] Katz, A.L., Webb, S.A., Committee on Bioethics, Macauley, R.C., Mercurio, M.R., Moon, M.R., Okun, A.L., Opel, D.J. and Statter, M.B., 2016. Informed consent in decision-making in pediatric practice. *Pediatrics*, *138*(2), p.e20161485.

[32] Keller, D., 2018. The right tools: Europe's intermediary liability laws and the EU 2016 general data protection regulation. *Berkeley Technology Law Journal*, *33*(1), pp.297-378.

[33] Kim, O.J., 2017. Ebbs and Flows: Issues in Cross-Border Exchange and Regulation of Health Information. *Annals Health L.*, *26*, p.39.

[34] Konduri, N., Aboagye-Nyame, F., Mabirizi, D., Hoppenworth, K., Kibria, M.G., Doumbia, S., Williams, L. and Mazibuko, G., 2018. Digital health technologies to support access to medicines and pharmaceutical services in the achievement of sustainable development goals. *Digital Health*, *4*, p.2055207618771407.

[35] Kulynych, J. and Greely, H.T., 2017. Clinical genomics, big data, and electronic medical records: reconciling patient rights with research when privacy and science collide. *Journal of Law and the Biosciences*, *4*(1), pp.94-132.

[36] Kyriazakos, S., Prasad, R., Mihovska, A., Pnevmatikakis, A., op den Akker, H., Hermens, H., Barone, P., Mamelli, A., De Domenico, S., Pocs, M. and Grguric, A., 2017. eWALL: An open-source cloud-based eHealth platform for creating home caring environments for older adults living with chronic diseases or frailty. *Wireless personal communications*, *97*, pp.1835-1875.

[37] Leenes, R., Palmerini, E., Koops, B.J., Bertolini, A., Salvini, P. and Lucivero, F., 2017. Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues. *Law, Innovation and Technology*, *9*(1), pp.1-44.

[38] Lloyd, M., 2018. Autonomy and paternalism in primary care. In *Primary care ethics* (pp. 25-39). CRC Press.

[39] Martin, T.J., Ranney, M.L., Dorroh, J., Asselin, N. and Sarkar, I.N., 2018. Health information exchange in emergency medical services. *Applied clinical informatics*, *9*(04), pp.884-891.

[40] McLoughlin, I.P., Garrety, K. and Wilson, R., 2017. *The digitalization of healthcare: Electronic records and the disruption of moral orders*. Oxford Univ

[41] McSwain, S.D., Bernard, J., Burke Jr, B.L., Cole, S.L., Dharmar, M., Hall-Barrow, J., Herendeen, N., Herendeen, P., Krupinski, E.A., Martin, A. and McCafferty, D., 2017. American Telemedicine Association operating procedures for pediatric telehealth. *Telemedicine and e-Health*, *23*(9), pp.699-706.

[42] Mello, M.M., ADLER-MILSTEIN, J.U.L.I.A., Ding, K.L. and Savage, L., 2018. Legal barriers to the growth of health information exchange—boulders or pebbles?. *The Milbank Quarterly*, *96*(1), pp.110-143.

[43] Mendelson, D., 2017. Legal protections for personal health information in the age of Big Data–a proposal for regulatory framework. *Ethics, Medicine and Public Health*, *3*(1), pp.37-55.

[44] Moon, L.A., 2017. Factors influencing health data sharing preferences of consumers: A critical review. *Health policy and technology*, *6*(2), pp.169-187.

[45] Mostert, M., Bredenoord, A.L., Biesaart, M.C. and Van Delden, J.J., 2016. Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. *European Journal of Human Genetics*, *24*(7), pp.956-960.

[46] Murray, E., Hekler, E.B., Andersson, G., Collins, L.M., Doherty, A., Hollis, C., Rivera, D.E., West, R. and Wyatt, J.C., 2016. Evaluating digital health interventions: key questions and approaches. *American journal of preventive medicine*, *51*(5), pp.843-851.

[47] Mustapha, A.Y., Chianumba, E.C., Forkuo, A.Y., Osamika, D. and Komi, L.S., 2018. Systematic review of mobile health (mHealth) applications for infectious disease surveillance in developing countries. *Methodology*, *66*.

[48] Norris, S.P. and Bain, L. eds., 2016. *Assessing the Impact of Applications of Digital Health Records on Alzheimer's Disease Research: Workshop Summary*. National Academies Press.

[49] Nusbaum, L., Douglas, B., Damus, K., Paasche-Orlow, M. and Estrella-Luna, N., 2017. Communicating risks and benefits in informed consent for research: a qualitative study. *Global qualitative nursing research*, *4*, p.2333393617732017.

[50] Ogungbenle, H.N. and Omowole, B.M., 2012. Chemical, functional and amino acid composition of periwinkle (Tympanotonus fuscatus var radula) meat. *Int J Pharm Sci Rev Res*, *13*(2), pp.128-132.

[51] Ohmann, C., Banzi, R., Canham, S., Battaglia, S., Matei, M., Ariyo, C., Becnel, L., Bierer, B., Bowers, S., Clivio, L. and Dias, M., 2017.

Sharing and reuse of individual participant data from clinical trials: principles and recommendations. *BMJ open*, *7*(12), p.e018647.

[52] Ostherr, K., Borodina, S., Bracken, R.C., Lotterman, C., Storer, E. and Williams, B., 2017. Trust and privacy in the context of user-generated health data. *Big Data & Society*, *4*(1), p.2053951717704673.

[53] Parasidis, E., 2017. Clinical decision support: elements of a sensible legal framework. *J. Health Care L. & Pol'y*, *20*, p.183.

[54] Pilegaard, M., 2016. The ethics of informed consent: An applied linguistics perspective. *Medical discourse in professional, academic and popular settings*, pp.79-102.

[55] Politou, E., Alepis, E. and Patsakis, C., 2018. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of cybersecurity*, *4*(1), p.tyy001.

[56] Price, I.I. and Nicholson, W., 2017. Medical malpractice and black-box medicine. *Big Data, Health Law, and Bioethics (Cambridge University Press, 2018), U of Michigan Public Law Research Paper*, (536).

[57] Reichel, J., 2017. Oversight of EU medical data transfers–an administrative law perspective on cross-border biomedical research administration. *Health and technology*, *7*(4), pp.389-400.

[58] Roth, L., Bempong, D., Babigumira, J.B., Banoo, S., Cooke, E., Jeffreys, D., Kasonde, L., Leufkens, H.G., Lim, J.C., Lumpkin, M. and Mahlangu, G., 2018. Expanding global access to essential medicines: investment priorities for sustainably strengthening medical product regulatory systems. *Globalization and health*, *14*, pp.1-12.

[59] Rumbold, J.M.M. and Pierscionek, B., 2017. The effect of the general data protection regulation on medical research. *Journal of medical Internet research*, *19*(2), p.e47.

[60] Saiod, A.K., van Greunen, D. and Veldsman, A., 2017. Electronic health records: benefits and challenges for data quality. *Handbook of Large-Scale Distributed Computing in Smart Healthcare*, pp.123-156.

[61] Sawicki, N.N., 2016. Mandating disclosure of conscience-based limitations on medical practice. *American Journal of Law & Medicine*, *42*(1), pp.85-128.

[62] Scott, I.A., Sullivan, C. and Staib, A., 2018. Going digital: a checklist in preparing for hospital-wide electronic medical record implementation and digital transformation. *Australian Health Review*, *43*(3), pp.302-313.

[63] Spencer, K., Sanders, C., Whitley, E.A., Lund, D., Kaye, J. and Dixon, W.G., 2016. Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: a qualitative study. *Journal of medical Internet research*, *18*(4), p.e5011.

[64] Sullivan, C., Staib, A., Ayre, S., Daly, M., Collins, R., Draheim, M. and Ashby, R., 2016. Pioneering digital disruption: Australia's first integrated digital tertiary hospital. *Medical Journal of Australia*, *205*(9), pp.386-389.

[65] Sund, K.L. and White, P., 2016. Precision Pediatric Genomics: Opportunities and Challenges. *Pediatric Biomedical Informatics: Computer Applications in Pediatric Research*, pp.295-312.

[66] Sundaravadivel, P., Kougianos, E., Mohanty, S.P. and Ganapathiraju, M.K., 2017. Everything you wanted to know about smart health care: Evaluating the different technologies and components of the internet of things for better health. *IEEE consumer electronics magazine*, *7*(1), pp.18-28.

[67] Syzdykova, A., Malta, A., Zolfo, M., Diro, E. and Oliveira, J.L., 2017. Open-source electronic health record systems for low-resource settings: systematic review. *JMIR medical informatics*, *5*(4), p.e8131.

[68] Tates, K., Antheunis, M.L., Kanters, S., Nieboer, T.E. and Gerritse, M.B., 2017. The effect of screen-to-screen versus face-to-face consultation on doctor-patient communication: an experimental study with simulated patients. *Journal of medical Internet research*, *19*(12), p.e421.

[69] Thomas, D., 2017. Advancing from Activated Patient to Autonomous Patient. *The Patient as Agent of Health and Health Care*, p.192.

[70] Thorogood, A., Mäki-Petäjä-Leinonen, A., Brodaty, H., Dalpé, G., Gastmans, C., Gauthier, S., Gove, D., Harding, R., Knoppers, B.M.,

Rossor, M. and Bobrow, M., 2018. Consent recommendations for research and international data sharing involving persons with dementia. *Alzheimer's & Dementia*, *14*(10), pp.1334-1343.

[71] Tresp, V., Overhage, J.M., Bundschus, M., Rabizadeh, S., Fasching, P.A. and Yu, S., 2016. Going digital: a survey on digitalization and large-scale data analytics in healthcare. *Proceedings of the IEEE*, *104*(11), pp.2180-2206.

[72] Tucker, K., Branson, J., Dilleen, M., Hollis, S., Loughlin, P., Nixon, M.J. and Williams, Z., 2016. Protecting patient privacy when sharing patient-level data from clinical trials. *BMC medical research methodology*, *16*, pp.5-14.

[73] Vayena, E. and Gasser, U., 2016. Strictly biomedical? Sketching the ethics of the big data ecosystem in biomedicine. *The ethics of biomedical big data*, pp.17-39.

[74] Vayena, E., Haeusermann, T., Adjekum, A. and Blasimme, A., 2018. Digital health: meeting the ethical and policy challenges. *Swiss medical weekly*, *148*, p.w14571.

[75] Wicclair, M.R., 2016. Conscientious objection. In *Encyclopedia of Global Bioethics* (pp. 729-740). Springer, Cham.