

# Bioethical aspects of telemedicine in Brazil: comprehensive analysis

Juracy Barbosa dos Santos<sup>1</sup>, Guilhermina Rego<sup>1</sup>, Rui Nunes<sup>1</sup>

1. Faculdade de Medicina da Universidade do Porto, Porto, Portugal.

## Abstract

Telemedicine has gained prominence in Brazil, especially in pandemic contexts and in remote areas. This article explores the bioethical and legal aspects of this practice, emphasizing the need for clear guidelines to ensure ethical and safe practice. This is a literature review focused on relevant publications addressing ethics, bioethics, information and communication technologies, data protection, and legal responsibilities associated with telemedicine. Various challenges and benefits of telemedicine were identified and analyzed, with emphasis on ethical issues, data protection, and legal responsibilities. Brazilian legislation was compared with international regulations. The results reinforce that the consolidation of telemedicine as a safe and socially legitimate practice depends on the integration of regulation, bioethical principles, and a continuous ethical commitment to patients' rights and well-being.

**Keywords:** Telemedicine. Bioethics. Computer security. Ethics, medical. Legislation. Brazil.

## Resumo

### Aspectos bioéticos da telemedicina no Brasil: análise abrangente

A telemedicina tem ganhado destaque no Brasil, especialmente em contextos de pandemia e áreas remotas. Este artigo explora os aspectos bioéticos e legais dessa prática, especialmente a necessidade de diretrizes claras para garantir uma prática ética e segura. Trata-se de revisão de literatura focada em publicações relevantes sobre ética, bioética, tecnologias da informação e comunicação, proteção de dados e responsabilidades legais associadas à telemedicina. Foram identificados e analisados diversos desafios e benefícios da telemedicina, com ênfase em questões éticas, proteção de dados e responsabilidades legais. A legislação brasileira foi comparada com regulamentações internacionais. Os resultados reforçam que a consolidação da telemedicina como prática segura e socialmente legítima depende da integração entre regulamentação, princípios bioéticos e compromisso ético permanente com os direitos e o bem-estar dos pacientes.

**Palavras-chave:** Telemedicina. Bioética. Segurança computacional. Ética médica. Legislação. Brasil.

## Resumen

### Aspectos bioéticos de la telemedicina en Brasil: análisis integral

La telemedicina ha ganado protagonismo en Brasil, especialmente en contextos de pandemia y en áreas remotas. Este artículo explora los aspectos bioéticos y legales de esta práctica, destacando la necesidad de directrices claras para garantizar una práctica ética y segura. Se trata de una revisión de la literatura centrada en publicaciones relevantes sobre ética, bioética, tecnologías de la información y la comunicación, protección de datos y responsabilidades legales asociadas a la telemedicina. Se identificaron y analizaron diversos desafíos y beneficios de la telemedicina, con énfasis en cuestiones éticas, protección de datos y responsabilidades legales. La legislación brasileña fue comparada con regulaciones internacionales. Los resultados refuerzan que la consolidación de la telemedicina como una práctica segura y socialmente legítima depende de la integración entre regulación, principios bioéticos y un compromiso ético permanente con los derechos y el bienestar de los pacientes.

**Palabras clave:** Telemedicina. Bioética. Seguridad computacional. Ética médica. Legislación. Brasil.

The authors declare no conflict of interest.

Telemedicine, defined as the use of information and communication technologies (ICT) for remote delivery of health care services, has been widely adopted in recent years as an innovative solution to various challenges in the health care sector. In Brazil, it has gained prominence as an essential tool for improving access to health care services, especially in remote areas, and for increasing efficiency in medical care. However, this practice raises important ethical questions that require careful consideration to ensure that telemedicine truly benefits patients and respects the fundamental principles of bioethics.

The rapid adoption of telemedicine in Brazil has led to several bioethical concerns, related to patient data privacy, quality of remote medical care, and equitable access to health care services. Authors such as Corrêa, Zaganelli, and Gonçalves<sup>1</sup> note that, despite technological advancements, ensuring that telemedicine does not compromise the quality of medical care and is used ethically and responsibly is fundamental. The focus of telemedicine must always be aligned with bioethical principles, prioritizing patient well-being and fair access to health care services<sup>2</sup>.

This study uses an exploratory and descriptive bibliographic approach to analyze bioethical issues associated with telemedicine in Brazil. The study is based on a review of current literature, with the objective of providing a comprehensive overview of the challenges and best practices for ethical implementation of telemedicine and reflecting on the effects of ICTs and globalization on health care from an ethical perspective, contributing toward the development of safer and more equitable practices in telemedicine.

## Method

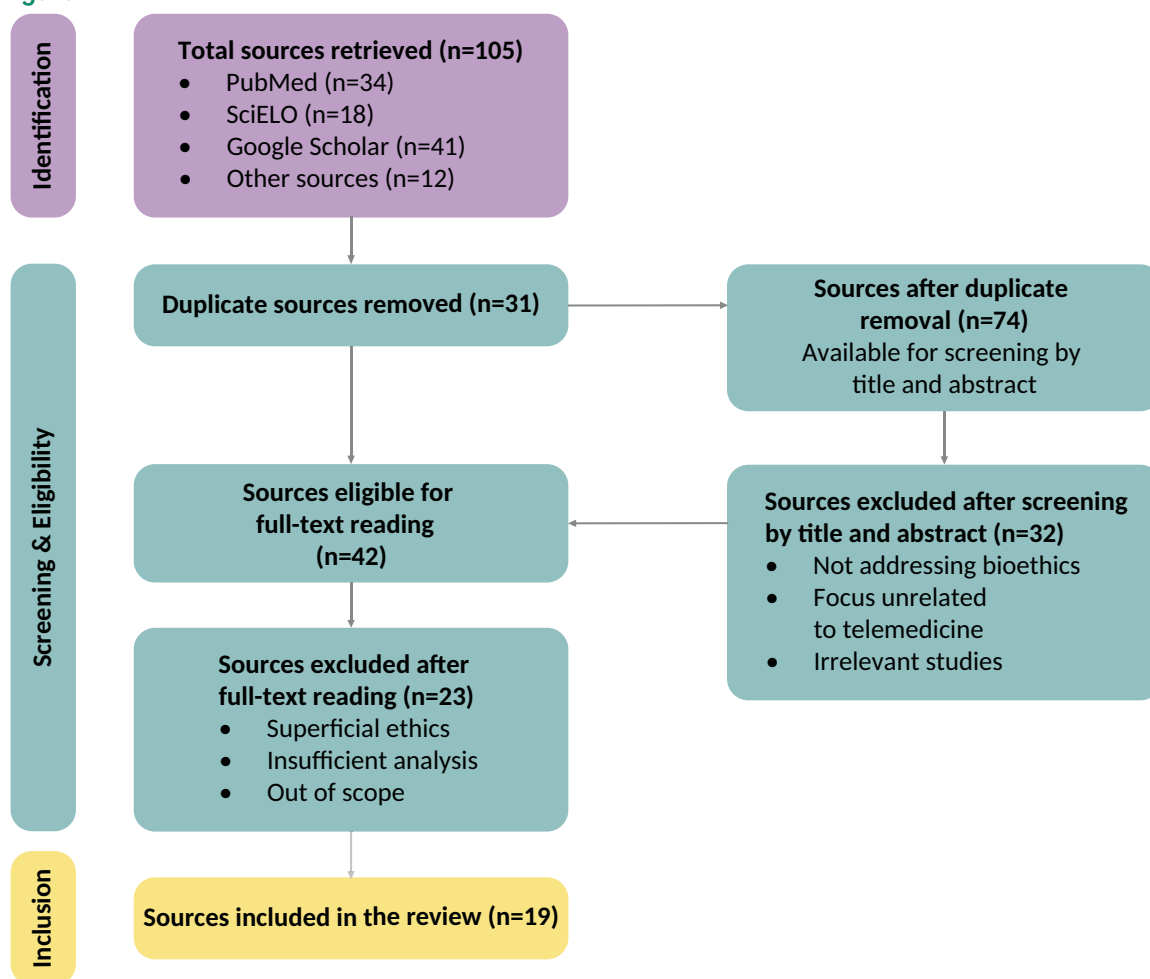
The methodological procedures followed the guidelines proposed by Köche<sup>3</sup> and by Prodanov and Freitas<sup>4</sup> for an exploratory and descriptive bibliographic review approach. The review adopted, in a guiding and deductive manner, the recommendations of PRISMA 2020<sup>5</sup>, aiming for transparency and logical organization of the source selection process, without aiming for strict systematicity.

The identification stage resulted in 105 records, from PubMed, SciELO, and Google Scholar databases, in addition to other relevant documentary sources, such as national and international legislations and institutional regulatory documents. After duplicate removal, 74 records were screened by title and abstract, and 32 were excluded for not addressing ethical or bioethical aspects, for presenting an exclusively technical focus, or for being unrelated to telemedicine.

In the eligibility phase, 42 documents were fully evaluated, of which 23 were excluded due to a superficial ethical approach, lack of structured bioethical analysis, conceptual redundancy, or inadequacy to the Brazilian or internationally compared scope. Finally, 19 studies composed the analytical body of the review, including scientific articles, legislation, theses, dissertations, and institutional documents, usually available in official gazettes and regulatory repositories. Data analysis and synthesis were critical and interpretative, providing the building of a systematized and well-founded understanding of the main bioethical aspects that permeate telemedicine in the Brazilian context.

Figure 1 presents the flowchart for the study identification, screening, eligibility, and inclusion process, conducted according to the PRISMA 2020 recommendations.

**Figure 1.** Search flowchart



## Discussion

### Definition of ethics and bioethics

Ethics is the branch of philosophy that studies the moral values and principles that govern human behavior in society. According to Araújo<sup>6</sup>, it refers to judgments about good and evil that guide human conduct, promoting personal and social well-being. It involves reflections on what is morally right or wrong, fair or unfair, in different contexts.

Bioethics is an extension of ethics focused on moral issues related to life and health. It is the study of the ethical dimensions of life sciences, encompassing views, decisions, conducts, and policies in these fields, seeking to guide practices that respect human dignity and rights<sup>7</sup>.

In traditional medical practice, ethics and bioethics guide the actions of health care professionals. Medical ethics, a subfield of professional ethics, assesses the risks, merits, and social impacts of medical activities, ensuring responsible practice and respect for patient rights and dignity<sup>8</sup>.

The fundamental ethical principles that guide medical practice include beneficence, non-maleficence, autonomy, and justice. Beneficence requires actions that promote health and well-being. Non-maleficence aims to avoid harm. Autonomy respects patient rights to informed decision-making, while justice demands equitable distribution of resources and treatments<sup>8</sup>.

The application of these principles in medical practice involves several responsibilities. Physicians

must clearly inform patients, ensure informed decision-making, preserve confidentiality, and treat everyone fairly, regardless of personal or socioeconomic factors<sup>8</sup>.

Bioethics, as a broader discipline, extends these principles to include concerns about social justice and equity in access to health care. It considers social and environmental conditions that impact health, advocating for integrated approaches. This includes assessing social determinants of health and advocating for policies that ensure equitable access to services for all<sup>7</sup>.

### Medical ethics in telemedicine

The ethical principles that constitute the foundation of traditional medical practice guarantee a relationship based on trust, respect, and justice. Beneficence requires physicians to prioritize patient well-being by treating and preventing illness and offering advice to improve quality of life<sup>2</sup>. Complementing beneficence, non-maleficence requires physicians to avoid causing harm by rigorously assessing the risks and benefits of interventions, thus ensuring that the benefits outweigh the risks<sup>2</sup>.

Autonomy recognizes the patient right to decide on their care. Physicians must provide clear and complete information, enabling informed decision-making. Respect for autonomy is essential for ethical and humanized practice<sup>2</sup>. Justice demands equity in resource distribution and equality in patient treatment, regardless of socioeconomic or personal factors. This approach promotes fair access to health care for everyone<sup>2</sup>.

These principles reinforce the trust between physicians and patients, which is essential for treatment adherence. Ethical medical practice also involves preserving patient confidentiality. This means that all patient personal and health information must be kept confidential, except when the patient consents to disclosure or when the law requires disclosure. Confidentiality is fundamental for building trust between physicians and patients<sup>2</sup>.

Finally, ethical practice requires professionalism and integrity. Physicians must treat everyone with dignity, communicate honestly, and avoid

discrimination or prejudice, promoting respectful and inclusive care<sup>2</sup>.

However, telemedicine has led to new ethical challenges, especially regarding patient data confidentiality. Electronic transmission increases the risk of privacy breaches, requiring platforms to adopt robust security measures to protect information<sup>1</sup>.

Informed consent also poses a challenge, as it is essential that patients understand the risks and benefits of treatments, which can be more difficult virtually. Physicians must explain treatments in detail and ensure space for questions and concerns<sup>9</sup>.

The physician-patient relationship, which is fundamental in medical practice, can be harmed by technological mediation. Distance hinders empathic connection and trust, requiring that professionals make an effort to maintain clear and humanized communication, using resources that favor visual and auditory interaction<sup>2</sup>.

Another challenge is equitable access to telemedicine, as not everyone has access to quality technology or internet connection, which results in inequalities. Public policies must ensure that everyone, regardless of location or socioeconomic status, can use these services<sup>9</sup>.

Data security remains a priority, with platforms required to adopt strict standards such as encryption and multifactor authentication<sup>1</sup>. Finally, patient acceptance varies and physicians must respect their preferences and offer support to make telemedicine a viable and comfortable option<sup>9</sup>.

Addressing the ethical challenges of telemedicine and ensuring the preservation of traditional ethical principles requires specific guidelines for remote medical practice. First, telemedicine platforms must implement advanced cybersecurity resources, such as encryption, firewall, and multi-factor authentication, in addition to regular audits, to ensure the security and confidentiality of patient data, tracing and correcting vulnerabilities<sup>1</sup>.

The guidelines must ensure equitable access to telemedicine, with quality care for everyone, regardless of location or socioeconomic status, including technical support and equipment as needed<sup>1</sup>. Consequently, telemedicine must be continuously monitored to ensure

ethical standards and quality, including safety review, patient satisfaction assessment, and outcome review, with feedback systems for constant improvement<sup>2</sup>.

The adoption of advanced technologies can help improve the safety and effectiveness of telemedicine. This includes the use of artificial intelligence for diagnostic support, remote monitoring for continuous patient follow-up, and the integration of connected health devices. The guidelines must foster technological innovation, while ensuring that these technologies are implemented ethically and safely<sup>1</sup>.

Health care professionals also need continuous telemedicine training that covers technical, ethical, and communicational aspects, so as to ensure ethical and quality care. Institutions must offer regular refresher programs on technologies and guidelines. Furthermore, they must humanize telemedicine care using clear and empathetic communication; video calls help maintain visual and emotional connection, making the experience closer to in-person care<sup>9</sup>.

Transparency is fundamental for ethical telemedical practice. Patients must be informed about how their data will be used and protected, and any security incidents must be communicated clearly and promptly. Open communication helps build trust and ensures patient awareness of their rights and the protective measures in effect<sup>9</sup>.

Patients must be actively involved in the development and implementation of telemedicine services. This includes consulting them about their needs and preferences, incorporating their perspectives into service design, and providing adequate support to help them use telemedicine technologies. Patient involvement helps ensure that services are accessible, understandable, and appropriate to their needs<sup>2</sup>.

In turn, the informed consent process must be clear, documented, and ensure that patients understand the treatment, risks, rights, and use of data. Physicians must explain options and answer all questions<sup>9</sup>.

### Information technologies and impacts on medicine

The evolution of ICTs has profoundly transformed medicine, providing new health care diagnostics,

treatment, and management tools and methods. Since the 1960s, ICTs have advanced from efficient administrative tools to clinical decision-making support, electronic health record, and telemedicine systems<sup>8</sup>.

Digital records have facilitated access to and exchange of information among professionals, improving the continuity and quality of health care<sup>7</sup>. Telemetry and remote monitoring systems have enabled remote follow-up, with faster and more personalized interventions<sup>7</sup>.

The COVID-19 pandemic increased the use of ICTs in medicine, showing the importance of digital solutions for maintaining health care services during social distancing. Remote consultations and treatments reduced infection risks and ensured the necessary care<sup>6</sup>.

The main technologies used in telemedicine include videoconferencing, digital platforms, and mobile devices. Video conferences are tools that enable remote consultations, diagnoses, and treatments in real time. They provide visual and auditory interaction, which are fundamental for building trust between physicians and patients<sup>10</sup>. Platforms such as Zoom, Microsoft Teams, and Google Meet are adapted to ensure privacy and meet the specific demands of the health care sector.

Digital health platforms provide functions such as scheduling, electronic records, secure communication, and access to medical information. These tools optimize health care management by facilitating information exchange and improving coordination among health care professionals<sup>8</sup>.

While devices such as smartphones and tablets are essential in telemedicine, as they enable patients to monitor their health in real time. Connected applications and devices, such as glucose meters and blood pressure monitors, assist in continuous monitoring and data collection, enabling more precise and personalized medical follow-up<sup>7</sup>.

ICTs provide several benefits to the medical field, such as improved accessibility to health care, especially for patients with reduced mobility or residing in remote areas. Telemedicine eliminates the need for travel, providing patients and professionals with time and resource savings<sup>10</sup>. Furthermore, these technologies facilitate

communication among health care professionals, promoting more integrated and efficient health care<sup>8</sup>.

Despite the benefits, ICTs pose challenges, such as patient data security and privacy. Digital information transmission increases the risk of cyberattacks and breaches, compromising confidentiality<sup>8</sup>. There are also concerns about inequalities in access, as patients lacking technological resources may be excluded<sup>6</sup>.

Adaptation to digital technologies is another barrier. Several health care professionals are not familiar with these tools, which can affect the effectiveness of care<sup>7</sup>. Remote consultations, although useful, face limitations, such as the impossibility of performing physical examinations, which can impact diagnoses and treatments.

### Data in virtual health environments

The protection of patient health data is crucial for trust in the digital health system and compliance with regulations such as the General Data Protection Law (LGPD) in Brazil and the Health Insurance Portability and Accountability Act (HIPAA) in the United States<sup>8</sup>. For prevention of unauthorized accesses and cyberattacks, resources such as encryption, multifactor authentication, firewall, and continuous monitoring are essential<sup>10</sup>.

Telemedicine platforms must strictly comply with legal security and privacy standards. In parallel, it is essential to foster a security culture among health care professionals through regular training and awareness-raising on data protection<sup>7</sup>. Transparency toward patients about how their data will be used and protected is also essential for preserving trust in the digital health system.

The responsibility for data security must be shared among technology developers, health care institutions, and physicians, with joint efforts to ensure safe and effective practices<sup>1</sup>.

### Aspects of the General Data Protection Law

The General Data Protection Law (LGPD) establishes a legal framework for the processing of personal data in Brazil, applying to both

natural and legal persons, public or private. In telemedicine, in which sensitive health data is processed, the LGPD plays an essential role, requiring strict protection and security<sup>11</sup>.

Telemedical personal data processing must comply with the LGPD principles, such as purpose, transparency, security, and accountability (art. 6)<sup>11</sup>. These principles guide ethical and secure data collection, storage, and use practices, fostering patient trust and legal compliance<sup>1</sup>. Informed consent is central, and must be free, explicit, and detailed, informing about data use purpose, sharing methods, and security measures (art. 7)<sup>11</sup>. This process educates patients about their rights and the importance of data protection<sup>1</sup>.

The LGPD requires additional protection for sensitive data, such as health information, due to the risk of discrimination in case of misuse. The processing of this data is permitted only with explicit consent or to protect the life or physical integrity of the data subject or third parties (art. 11)<sup>11</sup>.

Transparency is another key principle of the LGPD, which requires data controllers to provide clear and accessible information to data subjects about how their data is being used (art. 9)<sup>11</sup>. In telemedicine, this implies that patients are also informed about the rights they have, such as data access, rectification, erasure, and portability. Corrêa, Zaganelli, and Gonçalves<sup>1</sup> emphasize that transparency reinforces the relationship of trust between patients and health care providers.

Personal data processing in telemedicine must also include adequate security measures to protect data against unauthorized access, destruction, loss, alteration, communication, or any form of improper or unlawful processing (art. 46)<sup>11</sup>. These measures include the implementation of access controls, data encryption, and regular security audits. Responsibility is shared among companies, professionals, and technology developers<sup>1</sup>.

The appointment of a data protection officer (DPO) is mandatory to ensure compliance with the LGPD and assist patients and organizations as to questions and concerns (art. 41)<sup>11</sup>.

Finally, the LGPD provides for strict penalties for non-compliance, such as fines and data exclusion (art. 52), fostering compliance practices



and reinforcing public trust<sup>11</sup>. In telemedicine, adhering to the LGPD is vital to avoid sanctions and protect patients.

### Information security on telemedicine platforms

Information security is essential to protect patient data and ensure the reliability of telemedicine services. Platforms must implement robust measures to prevent unauthorized access, loss, alteration, or improper disclosure of data, ensuring legal compliance and user trust in the system<sup>2</sup>.

Encryption is an essential measure to protect data in transit and at rest, as it makes them inaccessible to third parties without the decryption key. This practice is fundamental for the protection of sensitive information, such as health data, during data transmission and storage<sup>2</sup>.

Access controls are also essential, as they limit access to authorized personnel only. Multifactor authentication, which combines methods such as passwords and codes sent to mobile devices, is crucial for preventing unauthorized access and cyberattacks, protecting the integrity of patient data<sup>9</sup>.

Regular security audits trace and correct vulnerabilities, ensuring compliance with regulations such as the LGPD. These audits keep the platforms updated and effective, reinforcing the security and reliability of the services<sup>2</sup>. Furthermore, continuous training for health care professionals is vital to foster a culture of safety. They must be prepared to recognize threats and protect data, ensuring practices consistent with organizational policies and regulations<sup>7</sup>.

Incident management is another pillar of security. Clear procedures for incident detection, response, and recovery minimize damage and ensure breach notification as required by the LGPD. A well-designed response plan reinforces patient confidence<sup>2</sup>.

Comprehensive security policies must be implemented to regulate all stages of data processing, from collection to deletion. Periodic reviews of these policies ensure their effectiveness in the face of changing threats or regulations<sup>1</sup>.

Collaboration among developers, service providers, and medical providers is essential

for integrating safety practices at all levels. Data protection is a shared responsibility that requires the commitment of all involved<sup>9</sup>.

Finally, transparency toward patients about adopted safety measures reinforces trust in the telemedicine system. Informing patients about the protection of their data and rights is a central aspect for safe and ethical practice<sup>2</sup>.

### Patient informed consent and privacy protection

Informed consent is a central principle of the LGPD and ethics in telemedicine. It must be free, informed, and unequivocal, so patients can understand how their data will be used, stored, and shared. The LGPD guarantees the right to clear information about the processing of personal data (art. 7, §1)<sup>11</sup>, requiring that patients be informed about the specific purpose, entities involved, and security measures adopted.

Obtaining informed consent is challenging, but essential for educating patients about their rights and data protection. Health care professionals must explain treatment options and risks, enabling informed decision-making. Furthermore, patients can revoke consent at any time, without prejudice to their care<sup>1</sup>.

Patient privacy is fundamental in telemedicine. Only authorized personnel should access patient data, exclusively for medical purposes. Any privacy violation must be handled with transparency, reinforcing ethics and trust in the system<sup>9</sup>. Telemedicine platforms need to adopt clear privacy policies, detailing data protection measures, patient rights, and violation reporting procedures. Transparency reinforces trust between patients and service providers<sup>2</sup>. Technical measures, such as encryption and strict access controls, are essential for protecting sensitive data. These practices ensure that patients share information with confidence<sup>2</sup>.

Regular training on informed consent and privacy protection is crucial for health care professionals. Data protection is a technical and ethical issue that requires the commitment of the entire team<sup>7</sup>.

Effective consent and privacy management includes an incident response plan, detailing data breach-related measures, such as immediate

notification to authorities and patients, as per the LGPD (art. 48) <sup>11</sup>. Effective incident management is crucial for preserving patient trust and the integrity of telemedicine services <sup>2</sup>.

Privacy must be prioritized at all stages of telemedicine platforms, from conception to operation. Developers, service providers, and medical professionals must adopt practices aligned with the best international guidelines and the LGPD. Privacy protection is a shared responsibility and essential for trust in services <sup>1</sup>.

### Theory of crime and imputation in telemedicine

The theory of crime in telemedicine applies criminal law principles to digital medical practices. Law 14,510/2022 <sup>12</sup> and the Federal Council of Medicine (CFM) Resolution 2,314/2022 <sup>13</sup> define guidelines for this practice, including criminal and civil liability of professionals. Imputation requires verifying criminal conduct, typicality, unlawfulness, and culpability.

Criminal conduct may include misdiagnoses, inappropriate prescriptions, and non-compliance with protocols. Typicality analyzes whether the conduct fits the criminal type, such as negligence, malpractice, and recklessness, punishable by the Brazilian Penal Code <sup>14</sup>.

Unlawfulness occurs when conduct is contrary to law, without legal justification, such as acting negligently and causing harm. Culpability assesses the professional's capacity to understand the illicit nature of an action and act accordingly, considering their preparation in digital technologies and telemedicine.

Objective imputation requires that the damage results directly from the physician's action or omission, establishing the causal link. CFM Resolution 2,314/2022 <sup>13</sup> requires strict adherence to protocols to ensure safety and effectiveness in care.

Law 14,510/2022 <sup>12</sup> notes the responsibility of professionals in telemedicine, reinforcing informed consent and transparency toward patients. It also provides for sanctions, including suspension or revocation of professional license, for those who fail to comply with legal standards.

Medical errors in telemedicine can lead to civil, criminal, and administrative liabilities. Civil

liability requires compensation for damages caused by negligence, recklessness, or malpractice, and professionals must ensure quality and safety in remote care, as per CFM resolution <sup>13</sup>.

Criminal liability covers offenses such as negligent bodily harm, negligent homicide, and failure to render aid, provided for in the Penal Code, which require proof of fault. Law 14,510/2022 <sup>12</sup> reinforces the need to comply with standards to avoid medical errors and their legal consequences.

In the administrative sphere, professional councils apply sanctions such as warnings, fines, suspension, and revocation of registration for those who fail to comply with ethical and technical standards of telemedicine, according to CFM resolution <sup>13</sup>. Rigorous adherence to these standards is crucial to ensure safe and effective remote care.

Professionals and institutions must adopt preventive measures, such as continuous updates in digital technologies, training, and quality and safety systems, as reinforced by the legal framework <sup>12,13</sup>, in order to minimize the risks of telemedicine.

Transparent communication with patients is essential. Professionals must clearly inform patients about the risks and benefits of remote care, ensuring informed consent, according to Law 14,510/2022 <sup>12</sup> and CFM Resolution 2,314/2022 <sup>13</sup>.

Breach of professional secrecy in telemedicine results in serious legal, ethical, and professional consequences for physicians and institutions. Professional secrecy is an ethical and legal duty that obliges professionals to maintain confidentiality on patient confidential information, as emphasized in CFM resolution <sup>13</sup>.

In the civil sphere, such violation can lead to compensation claims for moral and material damages, as patients have the right to reparation for unauthorized disclosure. Professionals and institutions must adopt measures to protect these data, as provided for in legislation <sup>12</sup>.

In the criminal sphere, such violation is a crime defined in the Penal Code (art. 154) <sup>14</sup>, with penalties of detention for three months to one year, or a fine. CFM Resolution 2,314/2022 <sup>13</sup> determines criminal and administrative sanctions for offenders. Administratively, the sanctions include warning, reprimand, suspension, and revocation



of registration, underscoring the need for strict adherence to ethical and legal principles in telemedicine<sup>13,14</sup>. In addition to sanctions, such violation compromises the trust between physician and patient, which is fundamental for therapeutic success and the integrity of medical practice, as noted by the CFM<sup>13</sup>.

Professionals and institutions must implement rigorous measures, such as the use of secure technologies, privacy policies, and regular training, in accordance with Law 14,510/2022<sup>12</sup> and CFM Resolution 2,314/2022<sup>13</sup>, to avoid violations. Transparency about information protection is vital for trust in telemedicine. Patients must be clearly informed about safety measures and their rights, ensuring open communication and privacy protection<sup>12,13</sup>.

The illegal practice of medicine via telemedicine represents a risk to public health and patient safety. The legislation establishes strict directives so only qualified and registered professionals can practice medicine through digital technologies<sup>12,13</sup>.

Illegal practice occurs when an unqualified or unregistered person provides consultations, diagnoses, prescriptions, or treatments without authorization. The Penal Code (art. 282)<sup>14</sup> provides for detention for six months to two years for this crime. Professionals must be registered with the CRM of their jurisdiction and comply with legal and ethical requirements. Health care institutions must ensure that only qualified professionals practice telemedicine<sup>13</sup>.

The consequences are severe: civil, criminal, and administrative sanctions. Patients can claim compensation for damages caused by illegal professionals, who can face imprisonment. Institutions that permit or facilitate illegal practice are also held administratively liable.

Institutions are responsible for ensuring that their platforms are used only by qualified professionals, with constant verification of records and security measures to prevent unauthorized access, as determined by law<sup>12</sup>.

### Regulation of telemedicine in the United States and the European Union

In the USA, data protection and telemedicine are regulated by federal and state laws.

The main federal legislation is the Health Insurance Portability and Accountability Act (HIPAA)<sup>15</sup>, enacted in 1996, which establishes national standards to ensure the privacy and security of patient health information<sup>15</sup>.

HIPAA requires covered entities, such as health plans, providers, and data intermediaries, to implement stringent measures, including encryption, access control, multi-factor authentication, and security audit. It also guarantees that patients can exercise the right to access and correct their information<sup>15</sup>.

For telemedicine, HIPAA imposes requirements to protect data during remote consultations, requiring that platforms ensure the security of electronic communications and patient data. Compliance is mandatory for all providers using digital technology<sup>15</sup>.

In addition to HIPAA, the Health Information Technology for Economic and Clinical Health Act (HITECH)<sup>16</sup> reinforces its provisions and promotes the use of electronic health records (EHR). HITECH provides for severe penalties for violations and requires notification to patients and the Department of Health and Human Services (HHS) in cases of significant breaches<sup>16</sup>.

The European Union (EU) has a harmonized approach to data protection and telemedicine regulation, based on the General Data Protection Regulation (GDPR)<sup>17</sup>, which came into force in May 2018. The GDPR establishes a comprehensive set of standards for the protection of personal data, applicable to all organizations that process data of EU citizens, regardless of where those organizations are located.

GDPR requires informed consent, transparency, and data minimization, and guarantees rights to data subjects, such as access, rectification, deletion, and portability. Organizations must adopt technical and organizational measures, such as pseudonymization, encryption, impact assessment, and breach notification within 72 hours<sup>17</sup>.

Regarding telemedicine, GDPR requires that service providers ensure that patient health information is processed with the utmost confidentiality and security. This includes the adoption of secure technologies for data transmission and storage, as well

as the implementation of clear policies and procedures for data protection. GDPR compliance is essential for any organization offering telemedicine services to EU citizens<sup>17</sup>.

In addition to GDPR, the EU has the NIS Directive<sup>18</sup>, which establishes requirements for the security of information networks and systems, including those used for the provision of health care services. The NIS Directive requires that operators of essential services, such as hospitals and clinics, implement adequate security measures and notify the competent authorities of any security incidents that may have a significant impact on the provision of services<sup>18</sup>.

The European Digital Health Strategy<sup>19</sup> also provides guidelines for the promotion of telemedicine and digital health in the EU. This strategy aims to improve the interoperability of health care systems, promote innovation in digital health, and ensure that digital health services are accessible and secure for all EU citizens. The strategy emphasizes the importance of data protection and privacy as foundations for citizen trust in digital health<sup>19</sup>.

### Comparison between Brazil, the United States, and the European Union

When comparing Brazilian legislation with US and EU regulations, it is observed that all three legal systems primarily aim to protect personal data and ensure security in the provision of digital health services. However, there are significant differences in the approaches and specific requirements.

In Brazil, the LGPD establishes comprehensive guidelines for the protection of personal data, applicable to all organizations that process the data of Brazilian citizens. The LGPD is similar to the EU's GDPR in terms of rigor and scope, requiring informed consent, transparency, and the implementation of adequate security measures. However, the LGPD presents peculiarities, such as the requirement for a DPO and specific sanctions for non-compliance with the rules<sup>11</sup>.

In the US, regulation is more fragmented, with HIPAA establishing federal standards for health data protection, complemented by state-specific telemedicine laws. HIPAA compliance is mandatory

for all health care providers, but enforcement and specific requirements may vary by state. The US approach is more practice-oriented and less centralized than the harmonized EU approach<sup>15,16</sup>.

The European Union, through the GDPR and the NIS Directive, adopts a highly regulated and harmonized approach to data protection and security in telemedicine. The GDPR imposes strict requirements for consent, transparency, and data security, applicable to all organizations that process the data of EU citizens. The EU digital health strategy also promotes interoperability and innovation, ensuring that digital health services are secure and accessible<sup>17,18</sup>.

In conclusion, although there are differences in approaches and specific requirements between Brazil, the USA, and the EU, all three legal systems recognize the importance of data protection and security in telemedicine. Compliance with local regulations is essential to ensure patient trust and effective digital health services. International best practices can serve as a benchmark for continuous improvement of data protection regulations and practices in telemedicine.

### Final considerations

The results of this exploratory and descriptive literature review indicate that telemedicine, in the Brazilian context, should be analyzed beyond its technical and regulatory aspects, requiring consistent ethical and bioethical reflection. The literature shows that the incorporation of ICTs in medical practice reconfigures the physician-patient relationship, health care, and sensitive data management, demanding a redefinition of classic bioethical principles.

Personal data protection arises as a central ethical aspect, directly associated with human dignity and the principle of non-maleficence. The analyzed studies indicate that confidentiality in the digital environment depends not only on legal compliance but also on the moral commitment of professionals and institutions to prevent risks and damages resulting from the misuse of health information. In this regard, the comparative analysis between Brazilian legislation and international frameworks shows convergence as to the centrality of privacy, although it underscores

that standards, by themselves, do not ensure ethically adequate practices.

As for autonomy, the literature indicates that informed consent in telemedicine should be understood as a continuous process of ethical communication, encompassing not only clinical aspects but also technological risks and data processing. Beneficence is associated with the potential to expand access to health care, while

justice imposes the need to address digital inequalities that can compromise the ethical indication of telemedicine.

Thus, the results reinforce that the consolidation of telemedicine as a safe and socially legitimate practice depends on the integration between regulation, bioethical principles, and a permanent ethical commitment to patient rights and well-being.

## References

1. Corrêa JCB, Zaganelli MV, Gonçalves BD. Telemedicina no Brasil: desafios ético-jurídicos em tempos de pandemia da Covid-19. *Humanit Tecnol (FINOM)* [Internet]. 2020 [acesso 21 maio 2025];25(1):200-18. Disponível: <https://bit.ly/4dHEuLw>
2. Garcia EF, Oliveira SM, Reis JG. Bioética e telemedicina. *Rev Bioética Cremego* [Internet]. 2020 [acesso 10 jun 2025];2(1):61-6. Disponível: <https://bit.ly/48Cxx4r>
3. Köche JC. Fundamentos de metodologia científica. Petrópolis: Vozes; 2015.
4. Prodanov CC, Freitas EC. Metodologia do trabalho científico. 2ª ed. Novo Hamburgo: Feevale; 2013.
5. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD *et al.* The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ* [Internet]. 2021 [acesso 18 maio 2025];372:71. DOI: 10.1136/bmj.n71
6. Araújo RCV. Direito versus bioética em tempos de pandemia: que desafios? *Rev Ang Ciênc Saúde* [Internet]. 2022 [acesso 21 maio 2025];1:1-4. DOI: 10.54283/RACSaude.v3i2supl1.2022.p1-4
7. Oliveira EL, Soares A, Lima J, Santos RM. Falhas de comunicação e epistemológicas limitam a abordagem da bioética na formação e na prática em saúde. *Interface (Botucatu)* [Internet]. 2021 [acesso 21 maio 2025];25:e200679. DOI: 10.1590/interface.200679
8. Cohen C, Gobbetti G, Oliveira RA. Breve discurso sobre ética, moral, estética e bioética das relações. *Rev Bras Psicanál* [Internet]. 2021 [acesso 21 maio 2025];55(2):41-57. Disponível: <https://bit.ly/4njFLN1>
9. Sánchez MVC, Costa FG, Bossio P, Fàbrega C, Abejas AG, Vergès AS. Telemedicina y eSalud: reflexiones desde la bioética. Barcelona: Institut Borja de Bioètica; 10 nov 2022. Disponível: <https://bit.ly/4wapuhs>
10. Sganzerla AS, Zanella DC, Paulo Neto A, Good C. A bioética como ética aplicada: a saúde em destaque. *Rev Inst* [Internet]. 2023 [acesso 21 maio 2025];5(2):59-78. Disponível: <https://bit.ly/4cZButq>
11. Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União* [Internet]. Brasília, nº 154-A, p. 1, 15 ago 2018 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4w7whs6>
12. Brasil. Lei nº 14.510, de 27 de dezembro de 2022. Altera a Lei nº 8.080, de 19 de setembro de 1990. Autoriza e disciplina a prática da telemedicina em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020. *Diário Oficial da União* [Internet]. Brasília, nº 244, p. 1, 28 dez 2022 [acesso 21 maio 2025]. Disponível: <https://bit.ly/42eG5mG>
13. Conselho Federal de Medicina. Resolução nº 2.314, de 20 de abril de 2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. *Diário Oficial da União* [Internet]. Brasília, p. 227, 5 maio 2022 [acesso 21 maio 2025]. Disponível: <https://tinyurl.com/hyrzwr3f>
14. Brasil. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. *Diário Oficial da União* [Internet]. Brasília, p. 23911, 31 dez 1940 [acesso 21 maio 2025]. Disponível: <https://bit.ly/3OJpDI1>
15. United States. Health Insurance Portability and Accountability Act (HIPAA). To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the

use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes. Federal Register [Internet]. Washington, 20 ago 1996 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4w9dEUT>

16. United States. Health Information Technology for Economic and Clinical Health Act (HITECH). Federal Register [Internet]. Washington, v. 74, n. 209, 30 out 2009 [acesso 21 maio 2025]. Disponível: <https://bit.ly/3QQVfMj>
17. European Union. General Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR). Off J Eur Union [Internet]. 2016 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4n6oRBj>
18. European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union. [Internet]. Brussels, 27 abr 2016 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4wbaiRe>
19. eHealth - digital services in health and care [Internet]. Brussels: European Commission; 2025 [acesso 21 maio 2025]. Disponível: <https://bit.ly/3OJpJzn>

**Juracy Barbosa dos Santos** – PhD student – [drjuracybarbosa@gmail.com](mailto:drjuracybarbosa@gmail.com)

 0009-0009-1729-9778

**Guilhermina Rego** – PhD – [guilherminarego@med.up.pt](mailto:guilherminarego@med.up.pt)

 0000-0002-8590-9832

**Rui Nunes** – PhD – [ruinunes@med.up.pt](mailto:ruinunes@med.up.pt)

 0000-0002-1377-9899

#### Correspondence

Juracy Barbosa dos Santos – Faculdade de Medicina da Universidade do Porto. Alameda Prof. Hernâni Monteiro, 4200-319. Porto, Portugal.

#### Contribution of the authors

Juracy Barbosa dos Santos: study conception; data analysis; manuscript writing. Guilhermina Rego: manuscript review. Rui Nunes: critical analysis; final manuscript review.

**Data availability:** All data used or generated in this study are described and presented in full in the body of the article.

**Editor in charge:** Dilza Teresinha Ambrós Ribeiro

**Received:** 4.28.2025

**Revised:** 6.5.2025

**Approved:** 1.13.2026