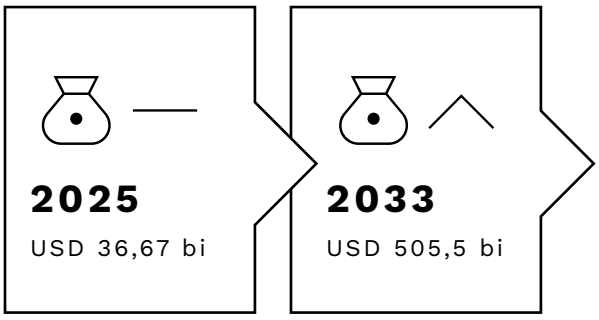
ARTIFICIAL INTELLIGENCE (“AI”) IN HEALTHCARE

Artificial Intelligence has profoundly transformed the healthcare sector, driving the development of technological solutions capable of monitoring, diagnosing, informing, and supporting clinical decision-making with increasing accuracy. These solutions span a broad spectrum of applications — from wearables devices and diagnostic imaging equipment to chatbots and virtual assistants designed to guide patients, organize health information, and support healthcare professionals and institutions.

According to the report ‘AI in Healthcare Market Size & Share | Industry Report, 2033’, the global AI in healthcare market was valued at approximately USD 36.67 billion in 2025 and is expected to reach USD 505.59 billion by 2033, growing at a compound annual growth rate of 38.90%.



In the international regulatory landscape, the World Health Organization (WHO) published, in 2023, the document Regulatory Considerations on Artificial Intelligence for Health, which establishes six key pillars for the regulation of AI in healthcare:

- documentation and transparency throughout the entire development process, to enable traceability of the stages and decisions adopted
- risk management and lifecycle oversight of AI systems, through an approach that encompasses everything from pre-market development to post-market surveillance and change management
- intended use and analytical and clinical validation, with transparent documentation and independent external validation calibrated to the level of risk of the application
- data quality and mitigation of bias and errors

privacy and data protection, with the implementation of compliance programs that take into account privacy and cybersecurity risks

engagement and collaboration among the different stakeholders involved

In a 2021 report entitled 'Ethics & Governance of Artificial Intelligence for Health', the WHO outlined the six consensus principles that should be observed to ensure that AI operates for the benefit of the population:

- protection of autonomy
- promotion of human safety and well-being
- ensuring transparency
- promoting accountability
- ensuring equity
- promoting responsive and sustainable tools

In Brazil, although the Artificial Intelligence Legal Framework (Bill No. 2338/2023) is still under discussion, the use of AI in healthcare is already supported by several regulatory instruments, particularly the following:

the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados - "LGPD"), which classifies health data as sensitive personal data, imposing stricter legal bases for its processing and prohibiting its sharing between data controllers for economic purposes;

ANVISA Resolution RDC No. 751/2022, which classifies software with clinical purposes as medical devices; and

Federal Council of Medicine ("CFM") Resolution No. 2,454/2026, which establishes rules for the research, development, governance, auditing, monitoring, training, and responsible use of AI solutions in medicine.

Considering this context, the Technology and Innovation team at Cescon Barrieu prepared this document with the aim of presenting the main benefits and risks associated with AI systems applied to healthcare, as well as the precautions that should be observed from a legal perspective, considering Brazilian legislation and different application formats.

1. MAIN APPLICATIONS AND BENEFITS OF AI TOOLS IN HEALTHCARE

Workflow automation: improved operational and administrative efficiency through the automation of workflows such as clinical notes-taking, appointment scheduling, billing, patient triage, clinical document management, authorization processing, and medical record summarization.

Robotic surgery: increased precision in surgical procedures, enabling fewer invasive techniques, telesurgery, and expanded access to healthcare.

Diagnostic and pharmacological support: analysis of large volumes of clinical data, laboratory tests, and medical images with high speed and accuracy, supporting healthcare professionals in diagnosis and in the precise prescription of medications and dosages, based on scientific evidence, clinical protocols, deep learning tools, and integrated patient data.

Monitoring and prevention: integration with health devices for continuous monitoring of clinical conditions, disease prevention, detection of infectious diseases, and support for clinical decision-making, as well as generating insights for chronic disease management and improved quality of life.

Information systematization: storage and analysis of large volumes of data, enabling the generation of clinical insights and a broader view of potential diagnoses and health conditions.

Virtual assistance and expanded access: use of chatbots, telemedicine, applications, and digital triage platforms capable of answering questions about medications and symptoms, providing health guidance, and supporting patient decision-making, helping bring healthcare services to regions with limited infrastructure or availability of specialized professionals.

2. MAIN RISKS RELATED TO THE USE OF AI TOOLS

Data and privacy: risks associated with improper processing of sensitive personal data, cyberattacks exposing health information, and secondary use of clinical data for commercial purposes without proper transparency. For AI systems based on Large Language Models (“LLMs”), one risk is “prompt injection” – the insertion of malicious instructions to manipulate system behavior and trigger unintended actions — including the unauthorized extraction of confidential information, such as patient records, clinical histories, and proprietary system data processed within the model’s context.

Algorithm quality and reliability: algorithmic bias arising from poorly representative training data, potentially leading to less accurate diagnoses for minority groups or populations in developing countries; diagnostic errors with serious clinical consequences (false positives and false negatives), especially when models are applied outside their training context; and hallucinations in language models, producing plausible but incorrect outputs.

Accountability and ethics: the complexity of many algorithms, especially those based on deep learning, makes it difficult to understand how decisions are made, raising concerns about reliability, auditability, and transparency regarding how clinical decisions are made by algorithms (the “black box” effect); risk of transferring complex medical decisions to automated systems without adequate human supervision; and potential harm to patient autonomy in the decision-making process.

Regulation and governance: limited number of countries with specific national strategies for AI in healthcare; lack of unified international standards for system certification and auditing; and challenges in rigorous clinical validation prior to large-scale adoption.

Systemic and operational risks: technical failures in critical clinical decision-support systems; dependence on technological infrastructure; rapid model obsolescence without proper retraining and validation processes; and misuse of AI by malicious actors for more sophisticated fraud within the context of health insurance plans and providers.

3. LEGAL CONSIDERATIONS FOR THE USE OF AI TOOLS

The obligations applicable to AI stakeholders vary depending on their role in the system’s value chain. For greater alignment with the Brazilian regulatory landscape, the definitions provided in Bill No. 2338/2023 (even though not yet in force) are adopted: (i) developer, a natural or legal person, public or private, who develops an AI system, directly or on demand, for market placement or application in a service provided under its own name or brand, whether for a profit or not; (ii) distributor, a natural or legal person, public or private, who makes an AI system available and distributes it for third-party use, whether for profit or not; and (iii) deployer (or user), a natural or legal person, public or private, who uses or applies an AI system on their own behalf or benefit, including configuring, maintaining, or supporting it through data provision for its operation and monitoring.

	DEVELOPER	DISTRIBUTOR	USER
LGPD	X	X	X
BILL NO. 2338/2023	X	X	X
ANVISA RDC RESOLUTION NO. 751/2022	X	X	-
CFM RESOLUTION NO. 2454/2026	X*	X*	X

*applicable indirectly via compliance requirements

3.1. BRAZILIAN GENERAL DATA PROTECTION LAW (LAW NO. 13,709/2018)

The LGPD applies to any processing operation involving personal data carried out by a natural or legal person, whether public or private, regardless of the means, the country of origin, or the location of the data, provided that the processing takes place in Brazil, the data collection occurs in Brazilian territory, or the data subjects are individuals located in Brazil. Accordingly, its obligations extend to developers, distributors, and deployers of AI systems.

In the context of AI systems applied to healthcare, its applicability is particularly relevant: the development, distribution, and use of these solutions invariably involve sensitive personal data — such as medical records, diagnoses, test results, and clinical histories — which receive heightened protection under the law. This means that the entire AI-in-healthcare chain, from training models on patient databases to generating real-time clinical recommendations, is subject to the LGPD's requirements, including the need for an adequate legal basis, the adoption of security measures proportionate to the sensitivity of the data, and the assurance of data subjects' rights, such as access, rectification, and review of automated decisions.

With respect to legal bases, the use of AI in healthcare presents additional challenges, as the processing of sensitive personal data is only permitted under the specific circumstances set forth in Article 11 of the LGPD. Therefore, all processing activities — from model training to their use for diagnostic or administrative purposes involving the sharing of health information — must be grounded in one of the legal bases provided for in that provision. The following are among the most applicable bases for potential uses in the healthcare field:

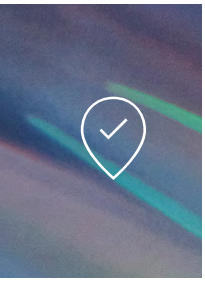
LEGAL BASIS

CONSENT

Specific and explicit consent, for defined purposes

APPLICABILITY IN AI IN HEALTHCARE

Requires the data subject to understand that their data will be processed by an AI system; must be granular and revocable; requires management mechanisms enabling revocation



LEGAL BASIS

EXERCISE OF RIGHTS

Including contractual contexts

APPLICABILITY IN AI IN HEALTHCARE

Applicable when data processing is strictly necessary for the performance/fulfilment of a contract

LEGAL BASIS

PROTECTION OF LIFE

Generally applicable in emergency situations

APPLICABILITY IN AI IN HEALTHCARE

Applicable in triage and emergency systems

LEGAL BASIS

PROTECTION OF HEALTHCARE

Exclusive to healthcare professionals, services, or health authorities

APPLICABILITY IN AI IN HEALTHCARE

Most common basis for clinical AI; processing must occur under the supervision of a healthcare provider

The development of machine learning systems presupposes, by definition, the need for training on datasets. When such data involve sensitive personal information — such as health data — the range of available legal bases narrows significantly: the use of legitimate interest as a legal basis is expressly prohibited, and the remaining applicable bases, such as health care, protection of life, and the regular exercise of rights, have limited scope and are unlikely to justify large-scale model training. In practice, the developer is left to rely on the data subject's consent — which, however, presents a technical and legal challenge with no easy solution: consent must be revocable at any time, but the technical means to "untrain" an already-trained model are, in the current state of technology, nonexistent, rendering effective revocation an obligation of uncertain compliance.

Furthermore, given that AI systems frequently operate through automated decisions, the agent must permanently and operationally ensure the possibility of human review of decisions affecting data subjects' interests.

The processing of health data by AI systems is inherently high-risk, making the preparation of a Data Protection Impact Assessment ("DPIA") essential. In the context of AI applied to healthcare, this report must go beyond a generic risk assessment and specifically address: (i) the risks of algorithmic bias with potential impact on diagnoses and treatments; (ii) the risks inherent in automated decisions

with direct effects on the data subject's health; (iii) the risks of data breaches with high discriminatory potential; and (iv) the auditability and traceability measures adopted in the system's processes.

It is also worth noting that, on February 25, 2026, the ANPD underwent a landmark institutional transformation: Law No 15.352/2026 formally converted the *Autoridade Nacional de Proteção de Dados* into a fully independent regulatory agency (*Agência Nacional de Proteção de Dados*), while granting it functional, technical, decisory, administrative, and financial autonomy.

Its enforcement powers were also significantly expanded: the agency's inspectors may now order the interdiction of establishments, equipment and facilities, as well as the seizure of goods and products, with the support of federal or state police in the event of resistance.

The law further created 200 specialized positions in data protection regulation and enforcement, to be filled by public competitive examination, substantially expanding the agency's technical and supervisory capacity. Against this backdrop of reinforced institutional standing, the ANPD has been actively shaping its regulatory and enforcement agenda with a specific focus on AI and health data.

The Regulatory Agenda 2025–2026 — published on December 11, 2024, by Resolution CD/ANPD No. 23/2024 — identifies artificial intelligence and sensitive data, including biometric and health data, among its 16 priority thematic areas for the normative phase.

More recently, the Priority Themes Map 2026–2027 — published on December 24, 2025, by Resolution CD/ANPD No. 30/2025 — lists AI and emerging technologies as one of its four central enforcement axes for the upcoming biennium. Together, these developments signal that the ANPD now has the institutional mandate, the enforcement tools, and the operational capacity to scrutinize LGPD obligations with unprecedented rigor, making proactive compliance a strategic priority for all agents across the healthcare AI chain.

PROHIBITIONS

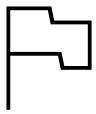
- selling, licensing or monetizing health databases;
- sharing health data with commercial partners in exchange for any form of compensation; and/or
- participating in data brokerage arrangements involving sensitive data.

3.2. AI LEGAL FRAMEWORK (BILL NO. 2338/2023)

The AI Legal Framework (if and when enacted) will establish a differentiated regime of obligations for AI systems classified as high-risk — a category that expressly includes applications related to diagnostic support and medical procedures. The AI Legal Framework distributes these obligations across the entire chain of agents involved in the development, distribution, and deployment of systems, with particular emphasis on traceability, bias mitigation, and algorithmic accountability.

GENERAL OBLIGATIONS	HIGH-RISK SYSTEMS (INCLUDES HEALTHCARE AI)
ALL AGENTS IN THE CHAIN	
• Ensure system safety and protection of affected individuals' rights • Cooperate with and provide information to authorities • Include an identifier in generated synthetic content • Report serious incidents to authorities	• Inform data subjects of procedures for exercising their rights • Report unexpected risks or impacts to the authority and other chain agents
DEVELOPERS	
• Prevent the use of systems for prohibited purposes • Publish summaries of protected content used in development • Compensate intellectual property rights holders whose works were used in training **GENERAL-PURPOSE AI SYSTEMS / GENERATIVE AI:** • Conduct preliminary risk assessments • Document models, tests, risks and datasets • Prepare technical documentation and usage instructions • Design systems sustainably • Cooperate in risk mitigation	• Maintain records of governance measures • Log system operations • Conduct security testing • Provide information to interpret generated results • Mitigate and prevent discriminatory biases • Share assessments with the sectoral authorities  Conduct an Algorithmic Impact Assessment

DEPLOYERS	
	• Document all stages of the system's lifecycle • Evaluate the results of the system's use • Document reliability and security testing • Document the degree of human oversight • Provide information to interpret results • Mitigate and prevent discriminatory biases Conduct an Algorithmic Impact Assessment
DISTRIBUTORS	
	• Support and verify compliance with governance measures by other chain agents



ALGORITHMIC IMPACT ASSESSMENT ("AIA")

Mandatory for developers and deployers. The AIA must identify, analyze, and mitigate algorithmic risks, including biases affecting diagnoses, automated decisions impacting health, and risks to vulnerable groups. Beyond risk mapping, the assessment must also address the technical dimensions of the system's development and deployment — in particular, the degree to which the tool is capable of providing explainability and transparency regarding its outputs and decision-making logic. This requirement presents a substantial practical challenge: as discussed above in the context of data and privacy risks, deep learning models are inherently opaque, making it difficult — and in some architectures, currently impossible — to fully account for how a given result was reached.

The AIA must therefore not only identify this limitation but also document the mitigation measures adopted, such as the use of post-hoc interpretability techniques, human oversight protocols, and the boundaries within which the system may be safely deployed. Developers must share assessments with the competent sector authority.

In the current version of the bill under consideration in the Chamber of Deputies, the ANPD will be responsible for coordinating the National System for the Regulation and Governance of Artificial Intelligence (SIA). The authority will have full normative, regulatory, supervisory, and sanctioning powers with respect to the development, implementation, and use of AI systems in economic activities that are not subject to oversight by a specific regulatory body or authority. In cases where a competent sectoral authority exists, the ANPD will act in a coordinated manner, providing technical support and serving an articulating role within the SIA. In this context, also within the scope of the AI Legal Framework, the ANPD's institutional influence is expanded, making the exercise of its enforcement powers even more significant.

3.3. ANVISA RDC NO. 751/2022 ("RDC 751")

RDC 751 establishes the risk classification rules, notification and registration regimes, and labeling requirements applicable to medical devices in Brazil. The regulation classifies as *Software as a Medical Device* ("SaMD") any software that performs medical functions independently — that is, without being incorporated into the hardware of a medical device — including mobile applications. Software limited to generic administrative, operational or informational functions remains outside the scope of RDC 751.

The determining criterion for this classification is the software's intended purpose. When designed for **diagnosis, prevention, monitoring, treatment** or **clinical decision support**, the system is considered a medical device and must be registered with the Brazilian Health Regulatory Agency ("Anvisa") prior to commercialization. Software intended exclusively for formal clinical investigations is exempt from notification or registration, provided it is not commercialized or used for other purposes. This exemption is not to be confused with the routine use of software by physicians for diagnostic support, which constitutes a direct medical purpose and subjects the system to registration as a SaMD.

The boundary between these categories, however, may be blurry. Anvisa may reclassify the product if it determines that an implicit medical purpose exists, even if not declared by the manufacturer.

RDC 751 classifies medical devices into four risk classes, which determine the applicable regulatory regime. Class I and Class II devices are subject to notification, while Class III and Class IV devices require prior registration with Anvisa.

For SaMDs, **Classification Rule 11** applies, which defines the regulatory classification according to the software's purpose and the potential clinical impact of the decisions it supports:

CLASS I
(LOW RISK)

REGULATORY REGIME

NOTIFICATION

EXAMPLE OF APPLICATION IN HEALTHCARE AI

Administrative software with no direct clinical impact, such as scheduling systems, hospital logistics management, or operational workflow organization

CLASS II
(MODERATE RISK)

REGULATORY REGIME

NOTIFICATION

EXAMPLE OF APPLICATION IN HEALTHCARE AI

Clinical decision support systems without immediate critical impact, such as test analysis tools or monitoring of non-vital physiological processes

CLASS III
(HIGH RISK)

REGULATORY REGIME

REGISTRATION

EXAMPLE OF APPLICATION IN HEALTHCARE AI

AI systems whose recommendations may influence critical clinical decisions, including software that assists with diagnoses that could lead to serious health deterioration or guide surgical interventions, as well as monitoring of critical vital parameters

CLASS IV
(MAXIMUM RISK)

REGULATORY REGIME

REGISTRATION

EXAMPLE OF APPLICATION IN HEALTHCARE AI

AI systems whose decisions or recommendations may result in patient death or irreversible health deterioration, such as algorithms used in highly critical clinical decisions

3.4. CFM RESOLUTION NO. 2.454/2026

CFM Resolution No. 2,454/2026 (“CFM AI Resolution”) establishes guidelines for the research, development, governance, auditing, monitoring and responsible use of AI systems in medicine. The regulation governs the use of these technologies in medical practice and structures a regulatory model based on human oversight, institutional governance and technological transparency.

The CFM AI Resolution rests on three central premises:

- Mandatory human supervision: AI is recognized exclusively as a support tool for medical practice. Physicians retain responsibility for clinical, diagnostic, therapeutic, and prognostic decisions and may not delegate such decisions to automated systems.
- Patient rights and autonomy: patients must be informed when AI systems are used as a material support in their care. The communication of diagnoses, prognoses or therapeutic decisions may not be carried out exclusively by automated systems, and patients retain the right to refuse the use of AI in their care.

- Institutional governance and risk assessment: healthcare institutions must implement internal governance mechanisms for the use of AI, including preliminary risk assessment, continuous monitoring of solutions, and the adoption of measures to prevent discriminatory biases, ensure transparency, and guarantee the protection of health data. In this regard, the CFM AI Resolution expressly reinforces the obligation to conduct an Algorithmic Impact Assessment. The document defines AIA as a continuous analysis of the impacts of an AI system, establishing that it "must be documented and periodically updated" with a view to identifying preventive and mitigating measures, directly aligned with the framework set forth in Bill No. 2,338/2023.

Although the CFM AI Resolution is directed primarily at physicians and healthcare institutions, its requirements produce significant indirect effects for AI technology developers and distributors, who are now expected to provide greater transparency, auditability, and interoperability in their systems.

Summary of obligations by agent:

KEY OBLIGATIONS / IMPLICATIONS

- Use AI systems exclusively as support tools
- Exercise critical clinical judgement over AI recommendations
- Record AI use in the patient's medical record
- Report failures or risks to competent authorities
- Stay informed about the capabilities, limitations and biases of systems
- Respect patient autonomy and rights

CONSEQUENCES OF NON-COMPLIANCE

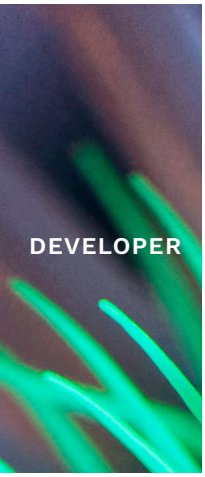
Ethical and disciplinary sanctions before the Regional Medical Council (Article 8), without prejudice to civil and criminal liability. The physician retains full responsibility for acts performed with AI assistance (Article 7).

KEY OBLIGATIONS / IMPLICATIONS

- Conduct preliminary risk assessment prior to adopting an AI solution
- Implement internal governance (transparency, auditing and bias mitigation)
- Establish an AI and Telemedicine Committee when using proprietary systems
- Ensure interoperability and continuous monitoring of solutions
- Ensure data protection and information security
- Collaborate with regulatory and supervisory bodies

CONSEQUENCES OF NON-COMPLIANCE

Oversight and supervision by the Regional Medical Council of the jurisdiction (Article 15). Failure to comply with governance obligations may give rise to administrative measures and liability of the technical director (Articles 9 and 14).

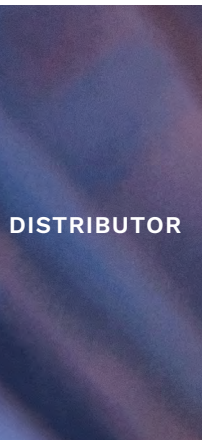


KEY OBLIGATIONS / IMPLICATIONS

- Provide clear technical documentation on the system's functioning, risks, and limitations
- Ensure auditability and explainability of solutions
- Adopt privacy by design and privacy by default principles
- Provide support for system updates, retraining, and monitoring
- Collaborate with regulatory authorities and healthcare institutions

CONSEQUENCES OF NON-COMPLIANCE

Indirect effects: systems that do not meet transparency, auditability, and explainability requirements may be refused or discontinued by medical institutions. Potential civil liability for failures attributable to the system (Article 7(2), read with applicable legislation).



KEY OBLIGATIONS / IMPLICATIONS

- Provide complete information about the distributed system
- Ensure the solution meets applicable regulatory and ethical requirements
- Act as intermediary between developer and medical institution
- Collaborate with institutions and oversight bodies in the event of incidents or failures

CONSEQUENCES OF NON-COMPLIANCE

Indirect effects: risk of system refusal or discontinuation by medical institutions if the solution does not meet regulatory and ethical requirements. Potential joint liability for failures in the supply chain, pursuant to applicable legislation.

Patients, as rights holders, are guaranteed: the right to information about the use of AI in their care; the right to refuse the use of AI systems; the right to privacy and confidentiality of their health data; the right to a second medical opinion; and the right to specific consent for experimental interventions.

The CFM AI Resolution creates a regulatory environment in which physicians and institutions will increasingly demand greater transparency, explainability, and security from technology providers. Developers and distributors who anticipate these requirements — incorporating them from the product conception stage — are likely to encounter fewer regulatory barriers and greater acceptance in the healthcare market.

4. CONCLUSION

Compliance with any of the legal instruments mentioned above does not substitute for, but rather supplements, the obligations set forth in the others. In practice, a single AI software solution may need to simultaneously comply with the following:

- notification or registration with Anvisa, according to its risk classification;
- compliance with the LGPD in the processing of health data, including an adequate legal basis, impact assessment, and limitations on data sharing;
- compliance with the AI Legal Framework, when it enters into force – or proactively, as a best practice measure; and
- adherence to the governance, auditing, and transparency requirements established by the CFM Resolution, which also sets forth its own risk classification for AI systems in medicine.

As regards potential liability, the irregular processing of personal data may give rise to administrative sanctions by the National Data Protection Agency ("ANPD") under the LGPD, while non-compliance with the AI Legal Framework will likewise subject the offender to the corresponding sanctions. The commercialization of software with a medical purpose without proper sanitary registration constitutes a sanitary infraction, subject to the penalties provided under applicable sector legislation, particularly Law No. 6,437/1977, while non-observance of CFM regulations may expose the physician to ethical sanctions before the Regional Medical Council, without prejudice to potential civil and criminal liability.

The combination of artificial intelligence and medicine is not only possible but highly promising. Those who choose to operate in this space, however, must be prepared to assume a structured, multi-layered regulatory burden — one that is actively enforced and continues to expand.

OUR TEAM

If you have any legal questions related to AI in HealthCare, please do not hesitate to contact our team:

ESTHER FLESCH
PARTNER
esther.flesch@cesconbarrieu.com.br

JULIA PAZOS
PARTNER
julia.pazos@cesconbarrieu.com.br

TANIA LIBERMAN
PARTNER
tania.liberman@cesconbarrieu.com.br

ANA LUIZA CALIL
OF COUNSEL
analuiza.calil@cesconbarrieu.com.br

PEDRO GUERRA
ASSOCIATE
pedro.guerra@cesconbarrieu.com.br

LAIS HORTA
ASSOCIATE
lais.horta@cesconbarrieu.com.br

ANA CAROLINA SCHINAIDER
ASSOCIATE
anacarolina.schinaider@cesconbarrieu.com.br