AI Governance Model,

Code of Ethics and Execution Framework

I. AI governance model

1. Necessity of Governance

The rise of Artificial Intelligence presents significant opportunities and cost-saving potential for organizations, driving its adoption across a multitude of sectors. However, integrating AI into products, especially medical devices, and internal processes without a robust governance framework exposes companies to considerable legal, financial, and reputational risks. Effective AI governance strikes a balance between fostering innovation and ensuring compliance with existing regulations, ethical standards, and commercial imperatives.

At Median Technologies, the Board of Directors and the appointed AI Committee are committed to establishing a comprehensive and adaptive AI governance framework that encompasses key elements such as the allocation of responsibilities and the implementation of AI governance tailored to the company's ethics and strategic objectives. This framework employs a risk-based approach that evaluates the likelihood and severity of potential harms associated with each AI use case, along with appropriate mitigation strategies.

2. Allocation of Responsibilities

Median and its Covered Persons are obligated to adhere to stringent anti-corruption laws worldwide, including (i) the French Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016, known as the "Sapin II Act", (ii) the United States Foreign Corrupt Practices Act (15

A successful AI governance framework relies on clearly defined roles, responsibilities, and decision-making processes. Assigning accountability ensures that AI initiatives align with organizational goals and established ethical standards.

i. **Board of Directors and Management:** The Board of Directors/Management are tasked with overseeing all major company initiatives, including those related to AI. This oversight involves understanding the potential risks associated with AI technologies and ensuring that effective governance frameworks are in place to mitigate these risks. The Board of Directors /Management's involvement is vital for aligning AI strategies with the Company's core values and objectives while setting a strong tone from the top. Given the strategic importance of AI literacy and continuous learning, the Board of Directors /Management will be regularly informed about developments in AI by relevant functions such as the AI Committee. Additionally, the AI Committee may decide to involve external experts or advisors to provide insights on the Company's AI governance strategy.

ii. **Management:** While the Board of Directors maintains ultimate oversight, the day-to-day management and operationalization of AI strategies are delegated to the AI Committee. They are responsible for developing and implementing AI policies, developing AI and/or integrating AI into business processes, and ensuring compliance with governance frameworks established by the Board/Management in accordance with the applicable laws. Monitoring adherence to regulations and internal policies will be delegated to the AI Committee. Management must

also evaluate the impact of AI on various business dimensions—such as efficiency, risk management, and competitiveness—and report these findings regularly to the Board of Directors /Management. Furthermore, management plays a crucial role in coordinating efforts across different organizational functions, working closely with the AI Committee to ensure alignment between AI initiatives and governance frameworks.

iii. **AI Committee:** An expert AI Committee has been established, comprising employees from diverse backgrounds including Information Technology (IT), Quality Assurance (QA), Finance, Legal Affairs (LA), Risk Management (RM), Regulatory Affairs (RA), Information Security (IS). Addressing governance issues related to AI requires a profound understanding of both technological contexts and legal/regulatory landscapes. The AI Committee will meet regularly to drive value-added implementation of AI within Median Technologies by:

- Mapping and monitoring how AI systems are developed, procured, and utilized internally.
- Developing internal guidelines and processes for deploying AI and creating use cases that incorporate best practices.
- Keeping the Board of Directors/ Management informed about technological advancements and regulatory changes.
- Conducting the Cost-Benefit Analysis (CBA) and Impact Assessment.
- Coordinating training for employees on the appropriate and effective use of AI.

The AI Committee may also seek external expertise as needed.

3. Reporting Structures and Escalation Pathway

Establishing clear reporting structures is essential for effectively implementing and maintaining AI governance. The AI Committee will maintain regular communication with the operational project functions, to provide guidance and support. In turn, the AI Committee will report consistently to the management and assist in their reporting obligations to the Board of Directors/Management regarding matters of AI governance.

Appropriate reporting and escalation will ensure that the AI Committee remain informed about performance metrics or issues related to AI systems. Risks or decisions must be addressed promptly at appropriate levels within the organization. Employees are encouraged to first report concerns to their supervisor or designated contact; if unresolved, issues should be escalated to AI Committee. For critical matters involving significant risks—such as legal, regulatory, or ethical concerns—the issue will be escalated by the AI Committee to the Board of Directors/ Management or, if the impact justifies it, external authorities.

This structured approach guarantees accountability, transparency, and efficient resolution of problems within our governance framework for artificial intelligence at Median Technologies.

This governance framework will undergo continuous evaluation and may be periodically updated in response to relevant regulatory, technological, and corporate developments.

II. AI Code of Ethics

1. Introduction

While AI is widely recognized for its transformative potential, studies consistently underscore the ethical, legal, and economic challenges it presents, particularly concerning human rights and fundamental freedoms. Notably, AI may pose significant risks to personal data protection and privacy and raise concerns about potential discrimination, especially when algorithms are applied in areas such as profiling and personal health information.

Equally concerning are the implications of AI and robotics on the labor market, with automation threatening the displacement of jobs. Additionally, there is a growing pressure to evaluate the impact of algorithms and automated decision-making systems in critical contexts, such as device safety, liability issues, and the execution of social and health policies, including patient safety.

In response to these challenges, Median Technologies acknowledges the imperative to embed ethical considerations throughout the AI lifecycle. Median Technologies is committed to harnessing AI's capabilities in a manner that adheres to the highest ethical standards. Fully aligned with the national, European Union and international 's regulatory framework, including the principles set forth in the AI Act, Median Technologies embraces the EU's ethical guidelines on AI, translating them into actionable day to day practices.

This AI Code of Ethics aims to guide the development and deployment of AI technologies in a way that ensures they are trustworthy, equitable, and ultimately beneficial to society.

2. Commitment

Median Technologies is committed to leveraging artificial intelligence (AI) to advance healthcare and medical imaging solutions while adhering to the highest ethical standards. This document reflects our corporate values, goals, and principles guiding the development, deployment, and use of AI technologies, models, and systems.

3. Corporate Values

Integrity: We ensure honesty and transparency in all our AI-related activities.

Innovation: We are committed to pioneering groundbreaking advancements that benefit society as a whole and individuals, particularly in healthcare, through the development of innovative AI/ML medical imaging technologies and software as a medical devices (SaMD) that could significantly enhance global health outcomes.

Accountability: We take full responsibility for the ethical and legal implications of our AI systems. Our commitment extends to strict compliance with all relevant laws, regulatory obligations, and technical standards required by applicable medical device regulations.

Respect: We prioritize respect for human rights, patient health, and data privacy in all our operations.

Collaboration: We engage with stakeholders, including healthcare professionals, regulators, and patients, to align our AI efforts with societal needs.

4. Our Goals

i. Advancing Healthcare:

- Deploy proprietary artificial intelligence, computer vision, and signal processing technologies to design and deliver software, imaging tests and services, addressing life-threatening unmet medical needs.
- Promote the use of AI to drive precision medicine and early disease detection.

ii. Customer Satisfaction:

- Ensure maximum customer satisfaction through personalized AI solutions and excellent support.

iii. Building Trust:

- Maintain transparency in AI decision-making processes to build trust among stakeholders.
- Communicate openly about the benefits, limitations, and potential risks of AI.

iv. Ensuring Ethical AI Use:

- Establish frameworks to ensure ethical AI practices across the company.
- Encourage stakeholder collaboration to align AI applications with societal needs.

v. Empowering Employees:

- Provide ongoing training and resources to employees to foster AI literacy and ethical awareness.
- Encourage employees to identify and report ethical concerns related to AI, and to use AI responsibly.

vi. Continuous Improvement:

- Regularly review and update AI policies and practices to reflect emerging technologies, laws, and ethical standards.
- Engage in research to develop innovative AI solutions while maintaining ethical integrity.

5. Our Key Principles in the Development and Deployment of AI Solutions

i. Human-centric Approach:

- We ensure that AI systems developed or deployed by Median Technologies are designed with human oversight and control, allowing for intervention and review of AI-driven decisions to maintain accountability and trust.
- Our AI technologies are developed with humans in the loop, ensuring that AI systems are transparent, explainable, and aligned with human values and ethical standards.

ii. Risk-Based Approach:

- Before we implement AI systems, we develop a clear understanding of potential risks of various natures and define appropriate mitigations.

- Risk assessments are conducted by the subject matter experts reviewed by the AI Committee throughout the AI lifecycle, including the development, deployment, and monitoring stages.

iii. Technical Robustness and Safety:

- We conduct thorough testing and vulnerability assessments to identify and mitigate potential cybersecurity risks, ensuring that our AI systems are secure and reliable throughout their lifecycle.
- We implement human-in-the-loop controls that allow operators to take over and abort AI functions in case of malfunctions or security breaches, maintaining safety and accountability.

iv. Compliance by Design and Default:

- All AI systems are designed to comply with applicable legal frameworks, including medical device regulations, GDPR, HIPAA, and AI-specific laws.
- Compliance is embedded in our processes, ensuring adherence to laws and ethical standards from inception.

v. Respect for Liabilities:

- The legal framework governing non-AI systems applies equally to AI, ensuring accountability and adherence to established liability standards.
- Our AI solutions are developed to meet strict safety and reliability criteria.

vi. Data Protection:

- We prioritize the security and privacy of all data, particularly sensitive and personal health information (PHI).
- Robust safeguards ensure data minimization, pseudonymization, and compliance with global data protection laws as applicable.

vii. Respect for Intellectual Property:

- We protect our intellectual property rights while avoiding infringement of third-party IP rights through rigorous due diligence and auditing.
- All AI innovations align with applicable IP frameworks to maintain fairness and legality.

viii. Respect for Humans and the Human Resources:

- Our AI systems support and increase human roles, avoiding bias or discrimination in hiring and employment decisions.
- Our AI systems do not replace human judgment in critical employment decisions.
- Our employees are empowered through training and awareness programs to understand AI's role and impact.

ix. Implementing Training and Literacy in AI:

- We encourage tailored training programs to enhance employees' understanding of AI technologies, ethical considerations, and responsible use, ensuring they are well-equipped to navigate the complexities of AI.
- We encourage continuous learning and provide specialized training for leaders on AI governance and ethics, fostering a culture of accountability and informed decision-making throughout the organization.

6. Conclusion

At Median Technologies, we are unwavering in our commitment to ethical and responsible AI development.

By adhering to this Code of Ethics, we do not only strive to create and deploy AI systems that respect human rights and comply with legal and regulatory standards but also aim to deliver transformative benefits to healthcare and society as a whole. Together, we will harness the potential of AI as a force for good: driving innovation, enhancing well-being, and respecting the health, safety, and fundamental rights of natural persons.

III. AI execution framework – operational guidelines

FRAMEWORK

In an era where artificial intelligence (AI) is rapidly transforming industries and redefining the landscape of business operations, organizations have the responsibility to establish clear and comprehensive guidelines governing the development, deployment, and usage of AI technologies.

At Median Technologies, we recognize that the potential of AI extends far beyond mere automation and cost-containment; it encompasses a spectrum of applications that can enhance decision-making, improve efficiency, and drive innovation. However, this potential can only be fulfilled if the use of AI is accompanied by a solid and ethical framework.

The ethical implications, regulatory requirements, and potential risks associated with AI necessitate a structured approach to ensure that our practices align with our corporate values and commitment to integrity.

We aim to empower our employees and management to harness AI's full potential while maintaining accountability and transparency in all AI-related activities.

This document outlines the guidelines for AI usage within our company, encompassing both:

- the development and deployment of proprietary AI systems, and
- the deployment (utilization) of third-party AI solutions, including off-the-shelf and open-source technologies.

These guidelines serve as a practical extension of the nine “Key Principles for the Development and Deployment of AI Solutions” outlined in the present AI Code of Ethics, ensuring their effective implementation. We believe they establish a robust framework that mitigates the risks of AI misuse while ensuring compliance with legal, regulatory and ethical standards, reinforcing our commitment to responsible AI practices in every project we undertake.

Critical aspects such as data privacy, security protocols, ethical considerations, intellectual property, and compliance with statutory requirements are encompassed.

Whatever we do, we shall remain vigilant in our adherence to these principles, fostering a culture of trust and excellence in all our endeavors related to AI. We expect continuous improvement and evolution in this sphere, driven by the practical experience gained within the Company. Our progress will align with evolving international standards and best practices in a field where technological advancements often outpace regulatory and legal frameworks.

Through these guidelines, Median Technologies seeks not only to lead in technological advancement but also to set a practical standard for ethical AI usage that aligns with our mission and values.

GUIDELINES

1. Human-Centric Approach

At Median Technologies, we embrace a human-centric approach to AI, fully aligning with the principles set out in the EU AI Act. This commitment ensures that our AI technologies and services are developed and deployed in a manner that upholds fundamental rights, promotes transparency, fosters accountability, and safeguards human oversight, fairness, and safety.

1.1. Key Elements of a Human-Centric Approach

i. **Human Oversight and Control:** We design our AI systems to ensure humans maintain oversight and control over AI-driven decisions. This includes implementing mechanisms for human intervention and review in the interest of accountability and trust.

ii. **Transparency and Explainability:** Our AI technologies are developed to be transparent and explainable, allowing users to understand how decisions are made. This transparency is crucial for building trust and ensuring that AI systems align with human values.

iii. **Clear Communication:** We maintain open lines of communication, ensuring that information about our AI systems is shared clearly and consistently, both internally and externally. This includes providing detailed documentation and explanations of AI decision-making processes.

iv. **Social Responsibility:** Our human-centric approach extends beyond our immediate stakeholders to the broader community. We strive to contribute positively to society by promoting ethical business practices and fostering sustainable development.

1.2. Implementation of the Human-Centric Approach

Do's:

- **Ensure Human Oversight:** Always maintain human oversight when using high-risk AI systems. Be prepared to intervene or override AI decisions as necessary.
- **Understand AI Limitations:** Familiarize yourself with the capabilities and limitations of the AI systems you work with to effectively monitor their operation.
- **Document Interventions:** Keep a record of any interventions made during the operation of AI systems, including the reasons for your actions according to Median Technologies' procedures.
- **Verify Outputs:** Before acting on outputs from high-risk AI systems, ensure that they have been verified and interpreted correctly.
- **Report Anomalies:** Promptly report any critical anomalies or unexpected behaviors hindering the use of the AI systems to your supervisor or the relevant IT team copying the AI Committee according to Median Technologies' procedures.

Don'ts:

- **Rely Solely on AI Decisions:** Do not depend entirely on AI-generated outputs without applying your judgment and expertise.

- **Ignore Training Needs:** Avoid neglecting opportunities for training on AI literacy and oversight responsibilities.
- **Withhold Information:** Do not keep concerns about AI system performance to yourself; communicate any issues or uncertainties to your team.
- **Disregard Safety Protocols:** Never bypass established protocols for intervention or emergency stop procedures when using high-risk AI systems**.**
- **Assume Compliance is Guaranteed:** Do not assume that following instructions alone will ensure compliance; actively engage in understanding how the system operates and its implications.

By embedding these principles into our AI systems, we prioritize ethical innovation that serves individuals and society while mitigating risks and ensuring compliance with evolving regulatory standards.

2. Risk-Based Approach in AI Development and Use

Effective AI governance demands strong risk management practices to identify, assess, and mitigate potential risks associated with AI implementation. This includes recognizing potential threats such as ethical breaches, and operational failures, and evaluating their potential likelihood and impact.

Risk management may include technical measures like data encryption and pseudonymization, alongside organizational actions such as corporate SOPs, employee training, and awareness programs. Additionally, an incident response plan must be relied upon to address AI-related incidents promptly, with the steps to be taken in the event of a data breach, serious incident, ethical violation, or other AI-related issues.

Risk assessment and management are particularly critical in the following areas: data protection and cybersecurity, intellectual property rights, and employment-related matters.

At Median Technologies, we adopt a risk-based approach in the development and deployment of AI technologies. This principle is central to our corporate philosophy, ensuring that we manage risks effectively while fostering innovation and efficiency.

2.1. Key Elements of a Risk-Based Approach

i. **Risk Identification:** We systematically identify potential risks associated with AI systems, including those related to security, privacy, and potential discrimination. This involves assessing the impact of AI on individuals, communities, and the environment using appropriate corporate tools and expertise.

ii. **Risk Assessment:** Once risks are identified, we conduct thorough assessments to evaluate their likelihood and potential impact. This process helps prioritize risks and allocate resources effectively for mitigation.

iii. **Risk Appetite:** Following the AI risk classification outlined in the AI Act, we do not develop or deploy AI systems classified as unacceptable risk. If the AI systems to be developed or deployed fall into the high-risk category, we shall implement all required controls, mitigations, and compliance measures to manage and mitigate risks, including conducting a FRIA and a DPIA, where applicable.

iv. **Risk Mitigation:** We implement robust measures to mitigate identified risks, ensuring that AI systems are designed to be safe, reliable, and compliant with regulatory standards and

applicable laws. This includes testing, validation, and continuous monitoring of AI performance.

v. **Continuous Monitoring:** Particularly, our risk management framework includes ongoing monitoring to ensure that AI systems continue to operate within acceptable risk parameters, reporting negative impacts. This involves regular reviews and updates to risk management strategies as new information becomes available.

vi. **Regulatory Compliance:** We align our risk-based approach with regulatory frameworks, such as the EU AI Act, which categorizes AI systems based on risk levels. This ensures that our AI technologies meet or exceed legal requirements, particularly for high-risk applications.

2.2. Implementation of the Risk-Based Approach

Do's:

- **Identify Risks:** Actively participate in identifying potential risks associated with AI systems you work with, including security, privacy, and ethical concerns.
- **Assess Impact:** Regularly evaluate the likelihood and potential impact of identified risks to prioritize them effectively.
- **Follow Guidelines:** Adhere to internal guidelines for risk management as outlined by the company, ensuring compliance with the EU AI Act.
- **Engage in Training:** Take part in training sessions related to risk assessment and management to enhance your understanding and capabilities.
- **Report Issues:** Promptly report any observed risks or incidents related to AI systems to your supervisor or designated risk management contact according to Median Technologies procedures.

Don'ts:

- **Ignore Risk Protocols:** Do not overlook established protocols for identifying and assessing risks associated with AI systems.
- **Assume All AI is Low Risk:** Avoid assuming that any AI system is low risk without conducting a proper assessment based on its intended use and potential impact.
- **Neglect Documentation:** Do not fail to document your findings related to risk assessments or any incidents involving AI systems.
- **Bypass Compliance Measures:** Never disregard compliance measures or guidelines set forth for high-risk AI systems; always follow them diligently.
- **Delay Reporting:** Do not delay reporting any risks or incidents; timely communication is essential for effective risk management.

By adopting a risk-based approach, Median Technologies aims to balance innovation with responsibility, ensuring that our AI technologies enhance lives while minimizing potential harm.

3. Respect for Technical Robustness, Safety, and Accuracy in AI Development and Use

At Median Technologies, we prioritize the principle of technical robustness, safety, and accuracy in the development and deployment of AI systems. These principles are essential for ensuring that our AI technologies are secure, reliable, and capable of functioning effectively throughout their entire lifecycle.

3.1. Key Elements of Technical Robustness, Safety and Accuracy

I. **Secure and Reliable Systems:** We design our AI algorithms and systems to be safe, transparent, secure and robust, and we put in place mitigations to account for the errors or inconsistencies that may arise during operation throughout the entire lifecycle. This includes implementing comprehensive cybersecurity measures to protect against unauthorized access, data breaches, and other cyber threats that could compromise system integrity. It will also involves training our users and providing clear, truthful and accurate information via supporting documentation.

II. **Data Quality and Bias Prevention:** In the interest of reliability and accuracy of the output, quality and integrity controls are implemented to minimize embedded bias, false positives, uncertainty, hallucinations, and inconsistencies. Third-party controls are also used to reduce design bias or misconceptions.

III. **Accuracy in AI-Driven Data Management:** Collecting accurate and up-to-date data to train the AI systems ensures that AI systems function correctly and make reliable decisions. When data used by AI is inaccurate or outdated, it can lead to faulty conclusions, poor decision-making, and potentially harmful outcomes:

   a. Data accuracy is a core principle in GDPR and AI, requiring businesses to regularly review and update the data used in AI processes. Ensuring accuracy means implementing robust data validation and QC monitoring procedures that detect errors and anomalies in the data input.

   b. For AI systems to comply with GDPR, HIPAA and AI regulations, they must be designed with mechanisms that continuously check data integrity. This reduces the risk of incorrect or biased decisions and strengthens trust in AI-driven processes.

IV. **Vulnerability Assessment:** We conduct thorough assessments of potential vulnerabilities when developing AI systems. This includes rigorous penetration and other testing to identify weaknesses that could be exploited by cyber-attacks or hacking attempts. By understanding these risks, we can implement appropriate safeguards to mitigate them.

V. **Logging and Traceability:** When developing AI systems, we implement logging features to allow traceability appropriate for the intended purpose of the system.

VI. **Human Control Mechanisms:** If an AI system is compromised or malfunctions, we ensure that human operators can take control and abort the system's functions. This human-in-the-loop approach is critical for maintaining safety and accountability in AI operations.

VII. **Collaboration with Security Experts:** We foster cooperation between our AI development teams and cybersecurity experts to enhance the resilience of our systems. This collaboration helps us stay informed about emerging threats and best practices for safeguarding our technologies.

VIII. **Compliance with Regulatory Standards:** We align our practices with the EU AI Act, which emphasizes the need for high-risk AI systems to achieve appropriate levels of accuracy, robustness, and cybersecurity. This includes ongoing monitoring and evaluation of system performance to ensure compliance with established standards.

3.2. Implementation of Technical Robustness and Safety Principles

Do's:

- **Ensure System Security:** Always implement security measures to protect AI systems from unauthorized access and data breaches.
- **Maintain Data Quality:** Regularly check and validate the quality of data used in AI systems to prevent bias and inaccuracies. The datasets used to (i) train/tune and (ii) test the algorithm must be pre-validated for statistical representativeness (likely large and high-quality training sets are preferable) and rigorously tested over a sufficient period to minimize embedded bias, false positives, uncertainty, hallucinations, and inconsistencies.
- **Perform Sandbox Testing:** Prior to deployment, the outcomes shall be assessed through simulations and testing in controlled environments.
- **Conduct Regular Testing and Auditing:** A robust testing and auditing framework that evaluates AI systems under various conditions must be implemented to ensure they perform reliably and securely, including output quality controls throughout the entire lifecycle.
- **Monitor System Performance Continuously:** Ongoing monitoring of AI systems must continue after deployment to identify any emerging issues promptly.
- **Conduct Cybersecurity Vulnerability Assessments:** Participate in assessments to identify potential vulnerabilities in AI systems and report any findings to the CISO.
- **Implement Logging Features:** Ensure that logging mechanisms are in place for traceability of AI system operations and default (e.g. “serious incidents”, as defined by the AI Act), required for accountability.
- **Stay Informed on Cybersecurity:** Collaborate with cybersecurity experts to understand emerging threats and best practices for safeguarding AI technologies.
- **Report Issues and Anomalies:** Promptly report any anomalies or unexpected behaviors in AI systems through the ticketing tool.

Don'ts:

- **Neglect Human Oversight:** Do not operate AI systems without ensuring that human oversight is in place to intervene if necessary.
- **Ignore Compliance Standards:** Avoid disregarding regulatory standards set forth by the EU AI Act regarding technical robustness and safety.
- **Overlook Testing Protocols:** Do not skip thorough testing of AI systems before deployment; ensure they perform reliably under various conditions.
- **Disregard Incident Response Plans:** Never ignore established incident response plans; always follow the steps outlined for addressing AI-related incidents promptly.
- **Assume Robustness is Guaranteed:** Do not assume that an AI system is inherently robust; actively engage in monitoring and improving its performance throughout its lifecycle.

By committing to technical robustness and safety in our AI development processes, Median Technologies aims to build trust with stakeholders, enhance user confidence, and ensure that our AI technologies are both effective and secure.

4. Compliance by Design and Compliance by Default in AI Development and Use

At Median Technologies, we adhere to the principles of Compliance by Design and Compliance by Default in the development and deployment of AI technologies. These principles are fundamental to our corporate philosophy, ensuring that our AI systems are inherently compliant with regulatory standards and ethical guidelines from the outset.

4.1. Key Elements of Compliance by Design

i. **Proactive Regulatory Alignment:** We integrate compliance with technical, legal, and ethical standards into every stage of AI development. This includes aligning with frameworks such as medical device regulations, as well as GDPR, HIPAA, and the EU AI Act to ensure that our AI systems meet or exceed regulatory requirements.

ii. **Risk Mitigation and Management:** Our development teams anticipate potential risks and implement comprehensive risk mitigation strategies. This involves understanding the ecosystem in which our AI systems operate, the applicable requirements, and addressing ethical considerations proactively.

iii. **Transparency and Accountability:** We design AI systems to be compliant, transparent, and explainable, ensuring that decision-making processes are clear and accountable. This includes providing detailed technical documentation and instructions to customers and ensuring traceability throughout the AI lifecycle. AI systems intended to directly interact with individuals must be designed to ensure that individuals are informed, as appropriate, that they are interacting with an AI system

iv. **AI Explainability:** Where relevant, research proposals should detail how the system's decision-making process will be made explainable to customers, ideally providing insights into why a particular decision was reached. Explainability is especially crucial for AI systems that make decisions, provide recommendations, or take actions that could cause significant harm, impact individual rights, or substantially affect individual or collective interests.

v. **Continuous Monitoring:** Post-market monitoring tools are integrated into our AI systems to track performance and identify potential risks or anomalies in real-time. This allows for timely updates and improvements based on user feedback and new data.

4.2. Key Elements of Compliance by Default

I. **Default Settings for Compliance:** Our AI systems are configured to operate in compliance with applicable laws and regulations as a default setting. This ensures that compliance is not an afterthought but an inherent part of how our systems function.

II. **Security and Privacy:** We prioritize data security and privacy, ensuring that AI systems protect sensitive information and adhere to privacy regulations by default.

III. **Ethical Considerations:** Ethical principles such as fairness, transparency, and accountability are embedded in our AI systems by default. This means that our AI technologies are designed to promote fairness and respect for human rights from the outset.

4.3. Implementation of Compliance by Design and by Default

Do's:

- **Integrate Compliance Early:** Ensure that compliance with medical device, legal, and ethical standards is considered at every stage of AI development, from conception to deployment.
- **Follow Regulatory Guidelines:** Familiarize yourself with relevant regulations such as medical device regulations, EU AI Act, GDPR, and HIPAA, and apply them to your work with AI systems.
- **Document Processes:** Maintain detailed documentation of AI development processes, including compliance measures taken and decisions made regarding ethical considerations.
- **Monitor Performance Continuously:** Engage in continuous monitoring of AI systems post-deployment to identify any compliance issues or anomalies promptly.
- **Prioritize Security and Privacy:** Implement security measures to protect sensitive data and PHI and ensure that privacy regulations are adhered to by default in all AI applications.

Don'ts:

- **Neglect Compliance Checks:** Do not overlook compliance checks during the development process; always ensure that your work aligns with established regulatory standards.
- **Assume Compliance is Automatic:** Avoid assuming that compliance will be achieved without proactive measures; actively engage in ensuring that systems are designed for compliance.
- **Ignore Ethical Considerations:** Do not disregard ethical principles such as fairness, transparency, and accountability when developing or deploying AI systems.
- **Bypass Documentation Requirements:** Never skip the documentation of compliance-related activities; thorough records are essential for demonstrating adherence to regulations.
- **Delay Reporting Issues:** Do not postpone reporting any compliance-related concerns or incidents; timely communication is critical for maintaining regulatory adherence.

By adopting compliance by design and default, Median Technologies aims to build trust with stakeholders, reduce regulatory risks, and ensure that our AI technologies are both innovative and responsible.

5. Respect for Liabilities in AI Development and Use

At Median Technologies, we recognize the importance of respecting liabilities in the development and deployment of AI technologies. This principle is crucial to our corporate approach, ensuring that we manage risks effectively and maintain accountability for the impact of our AI systems.

5.1. Key Elements of Respect for Liabilities

I. **Legal Framework Alignment:** Our AI development and deployment practices shall align with legal frameworks such as the EU's AI Liability Directive (AILD) and the Product Liability Directive (PLD). These frameworks provide a structured approach to managing liability risks associated with AI, ensuring that victims of AI-related damages receive fair compensation.

II. **Fault-Based Liability:** We operate under a fault-based liability framework, which requires demonstrating negligence or misconduct to establish liability. This approach encourages responsible AI development and use by emphasizing the importance of adhering to safety standards and best practices.

III. **Accountability and Transparency:** We acknowledge that AI systems can introduce unique challenges in establishing liability due to their complexity and potential for unforeseen outcomes. Therefore, we prioritize transparency in AI decision-making processes, ensuring that our systems are explainable and accountable.

IV. **Continuous Monitoring and Improvement:** We continuously monitor our AI systems for potential risks and update our practices based on new external and internal information, any new or updated regulations from legal/ regulatory (AI / cyber /medical devices...) watch. This proactive approach ensures that we remain compliant with evolving liability standards and maintain high levels of accountability.

5.2. Implementation of Respect for Liabilities

Do's:

- **Liability Management:** Validate the data used for proprietary algorithm training in terms of third-party liability and statutory liability to prevent disputes or violations regarding the legality of their use in both training and output generation; when procuring third-party AI systems for deployment, ensure in advance that contractual provisions with the supplier permit the safe and unrestricted use of outputs, without risking violations of confidentiality obligations, professional secrecy, or non-disclosure agreements. In case of doubt, you can contact the VP & General Counsel.
- **Maintain Transparency:** Ensure that AI systems are designed to be transparent. Document decision-making processes to facilitate accountability.
- **Report Incidents Promptly:** Immediately report any incidents or malfunctions of AI systems that could lead to liability issues to your supervisor or the relevant team.
- **Engage in Continuous Learning:** Stay informed about evolving liability standards and participate in training related to compliance and risk management in AI.

Don'ts:

- **Neglect Accountability:** Do not overlook your responsibility for the outcomes of the AI systems you work with; always consider the potential impact of your decisions.
- **Assume Compliance is Automatic:** Avoid assuming that your work is compliant without actively verifying adherence to legal standards and internal guidelines.
- **Delay Reporting Issues:** Never postpone reporting any potential liability concerns or incidents; timely communication is crucial for effective risk management.
- **Disregard Documentation Requirements:** Do not neglect the importance of documenting processes related to liability; thorough records are essential for demonstrating compliance and accountability.

By respecting liabilities in AI development and use, Median Technologies aims to build trust with stakeholders, reduce legal uncertainties, and ensure that our AI technologies are both innovative and responsible.

6. *Data Protection and Protection of Personal Health Information (PHI) in AI Development and Use*

At Median Technologies, we recognize the critical importance of protecting personal data, especially sensitive health information, in the development and deployment of AI technologies. This principle is integral to our corporate philosophy, ensuring that our AI systems respect privacy and adhere to stringent data protection standards.

6.1. Key Elements of Data Protection in AI

I. **Lawfulness, Fairness, and Transparency:** We ensure that all personal data processing by AI systems is lawful, fair, and transparent. This includes providing clear information about how data is used in AI-driven processes and AI systems and obtaining explicit data subject's consent, when necessary.

II. **Purpose Limitation and Data Minimization:** Our AI systems are designed to collect and process personal data only for specified, legitimate purposes. We adhere to the principle of data minimization, ensuring that only necessary data is collected and processed.

III. **Privacy by Design and Default:** We integrate data protection into AI systems from the outset, using privacy by design principles. Additionally, our systems are configured with privacy-friendly default settings to protect user data automatically.

IV. **Data Security and Confidentiality:** We implement robust security measures to protect sensitive data, including, as applicable: pseudonymization, encryption, access controls, and regular security audits. This ensures that personal health information remains confidential and secure.

V. **Data Retention and Deletion:** Our AI systems are designed to retain data only for as long as necessary for its intended purpose. Once the purpose is fulfilled, data is securely deleted or pseudonymized to prevent unauthorized access and breaches.

VI. **Report Issues:** Promptly report any observed risks for personal data or data breaches related to AI systems to your supervisor or designated data privacy contacts.

6.2. Protection of Personal Health Information (PHI)

I. **Specialized Safeguards for PHI:** We recognize that PHI requires additional protection due to its sensitive nature. Our AI systems handle PHI with particular care, using techniques such as anonymization and pseudonymization, as applicable, to reduce personal references.

II. **Explicit Consent for PHI Processing:** Explicit consent from individuals are collected and obtained by the competent third parties before processing their PHI, ensuring that they are fully informed about how their data will be used.

III. **Regular Training and Awareness:** Our employees undergo regular training on handling sensitive data, including PHI, to ensure they understand the importance of confidentiality and compliance with data protection regulations.

6.3. Implementation of Data Protection Principles

Do's:

- **Embed Data Protection in AI Development:** Ensure that data protection is integrated into every stage of AI development, from design to deployment by managing data privacy risks, and reducing the impact on affected data subjects.
- **Ensure Lawful Data Processing:** Always process personal data in a lawful, fair, and transparent manner. Obtain explicit consent when required.
- **Obtain Explicit Consent for PHI:** Always secure explicit consent from individuals before processing their personal health information, ensuring they are fully informed about its use.
- **Limit Data Collection and Use:** Collect and process only the personal data necessary for specific, legitimate purposes. Adhere to the principle of data minimization and avoid using personal data whenever possible.
- **Maintain Data Security:** Employ robust security measures, such as encryption, two-factor authentication, and access controls whenever possible and applicable, to protect sensitive data, including PHI and genetic data.
- **Ensure transparency:** Respect data subjects' rights by providing prompt and comprehensive follow-up to individuals requesting information about the processing of their data or seeking to block processing, update, or rectify their data, etc.
- **Participate in Data Privacy Training:** Engage in regular training on data protection and handling sensitive information to stay informed about compliance requirements.

Don'ts:

- **Ignore Transparency Requirements:** Do not fail to provide clear information about how personal data is used in AI systems; transparency is essential for building trust.
- **Neglect Training Data Compliance:** Do not use training data that is processed without a proper legal basis (e.g. consent) or without providing adequate information to the concerned data subjects.
- **Neglect Data Retention Policies:** Avoid retaining personal data longer than necessary for its intended purpose. Ensure secure deletion of data once it is no longer needed.
- **Bypass Security Protocols:** Never disregard established security protocols for handling sensitive data; always follow best practices to protect against breaches.
- **Process Data Without Consent:** Do not process personal health information, including for algorithm training, without obtaining the individual's explicit consent.
- **Overlook Compliance Obligations:** Avoid assuming that compliance with data protection regulations is automatic; actively verify that your practices align with legal requirements.

By prioritizing data protection and the safeguarding of personal health information, Median Technologies aims to build trust with stakeholders, reduce regulatory risks, and ensure that our AI technologies are both innovative and responsible.

7. Respect for Intellectual Property (IP) in AI Development and Use

At Median Technologies, we recognize the importance of respecting Intellectual Property (IP) rights in the development and deployment of AI technologies. This principle is crucial to our corporate philosophy, ensuring that our AI systems are developed and used in a manner that respects the creative and innovative contributions of others.

7.1. Key Elements of IP Respect in AI

i. **Protection of IP Rights:** We ensure that our AI systems do not infringe on existing IP rights, such as patents, copyrights, and trade secrets. This includes respecting the rights of third-party data providers and ensuring that AI training data is used legally and ethically.

ii. **Compliance with Copyright Laws:** Our AI development processes comply with copyright laws, particularly when using copyrighted materials for training AI models. We adhere to regulations like the EU Copyright Directive, which allows data mining for scientific purposes under certain conditions.

iii. **Transparency in AI Development:** We maintain transparency about the data and materials used in AI model training. This includes providing summaries of training data, as required by the EU AI Act while protecting trade secrets and confidential information.

iv. **Ownership and Licensing Agreements:** When collaborating on AI development, we establish clear ownership and licensing agreements to ensure that creators and contributors receive appropriate credit and compensation for their work.

v. **Respect for third-party IP rights**: There is a high risk of infringing third-party IP rights or violating confidentiality obligations when using generative AI applications. Therefore, caution is required when deploying Large Language Models (LLM) and third-party generative AI in this context. In case of doubt, please contact the VP Legal & General Counsel.

7.2. Implementation of IP Respect Principles

Do's:

- **Acknowledge IP Rights:** Always recognize and respect intellectual property rights in your work. Ensure that you have proper authorization before using or reproducing any materials.
- **Comply with Copyright Laws:** Familiarize yourself with and adhere to the principles of copyright laws, particularly when using copyrighted materials for training AI models. Exercise caution when selecting information as input for third-party AI applications and LLM (e.g. in your prompts). Avoid using data that is protected by third-party IP rights for which you lack a license, or that constitutes trade secrets or other confidential business information.
- **Maintain Transparency:** Be transparent and accountable about the data and materials used in AI model training. Provide clear summaries of training data as required, while protecting trade secrets.
- **Establish Ownership Agreements:** When collaborating on AI projects, ensure that clear ownership and licensing agreements are in place to give appropriate credit and compensation to creators. Where appropriate, contact the VP Legal & General Counsel.
- **Use Licensed Data:** Limit the use of generative AI applications and LLM to those which utilize data owned by the provider, public domain data, or data that has been appropriately licensed from third parties.
- **Protect your Data:** Be mindful that you may not be able to claim IP rights over work results derived from third-party generative AI applications and LLM. Consider using applications that operate on private cloud environments and review their settings to determine whether they permit the AI provider to store and train on user prompts. Whenever possible, seek appropriate legal protections

and assurances against the use, storage, and training of the AI on the Company's prompts to safeguard trade secrets and other confidential information.

- **Caution in Using AI-Generated Outputs:** Limit the application of generative AI and LLM to internal business use or for brainstorming purposes rather than creating final work products. If you choose to use generative AI for producing finished outputs, conduct thorough checks for potential IP infringements before commercial use. While many AI applications include integrated tools designed to prevent IP violations, these tools may not always be reliable.

Don'ts:

- **Infringe on IP Rights:** Do not use or incorporate materials that infringe on existing intellectual property rights, such as patents or trade secrets, without proper authorization.
- **Neglect Training Data Compliance:** Avoid using training data that is protected by third-party IP rights for which you do not have a license.
- **Assume Output Ownership Automatically:** Do not assume you will retain IP rights over outputs generated by AI applications and LLM; always review the terms of service regarding ownership.
- **Ignore Ethical Considerations:** Never disregard ethical considerations when using generative AI and LLM; ensure that your practices align with legal standards and respect for IP.
- **Bypass Internal Compliance Processes:** Do not overlook internal compliance procedures designed to minimize the risk of IP infringement; always follow established guidelines.

By respecting Intellectual Property rights in AI development and use, Median Technologies aims to foster a culture of innovation and collaboration, ensuring that our AI technologies are both groundbreaking and responsible.

8. Respect for Humans and Human Resources (HR) in AI Development and Use

At Median Technologies, we recognize the importance of respecting humans and human resources in the development and deployment of AI technologies. This principle is central to our corporate philosophy, ensuring that AI systems are designed and used in a way that enhances human capabilities, promotes well-being, and supports the development of our employees.

8.1. Key Elements of Respect for Humans and HR in AI

I. **Human-Centric Design:** Our AI systems are designed with a human-centric approach, focusing on enhancing human capabilities and improving lives. This includes ensuring that AI technologies are intuitive, accessible, and beneficial to customers.

II. **Employee Development and Training:** We prioritize the development and training of our employees, providing them with the skills needed to thrive in an AI-driven environment. This includes offering opportunities for continuous learning and professional growth.

III. **Transparency:** When deploying relevant AI systems at the workplace, workers' representatives and all affected workers shall be promptly notified.

IV. **Fair Labor Practices:** We adhere to fair labor practices, ensuring that the use of AI does not unfairly replace human labor but rather complements it. This involves implementing AI in a way that supports job creation and enhances work quality.

V. **AI & Employee Rights:** Median Technologies will not use AI systems or tools to conduct indiscriminate surveillance on our employees or to manage the employment relationships in an entirely automated manner, nor to make decisions that produce legal effects on employees or that may significantly affect them.

VI. **Human Oversight and Accountability:** We maintain human oversight and accountability in AI decision-making processes. This ensures that AI systems are transparent, explainable, and subject to human review and intervention when necessary.

8.2. Implementation of Respect for Humans and HR Principles

Do's:

- **Prioritize Human-Centric Design:** Ensure that AI systems are developed with human needs and well-being at their core.
- **Communicate Transparently:** Inform relevant workers' representatives and affected employees promptly when deploying AI systems that may impact their roles.
- **Support Fair Labor Practices:** Advocate for the use of AI that complements human labor rather than replaces it, promoting job creation and enhancing work quality.
- **Maintain Human Oversight:** Participate actively in decision-making processes involving AI systems, ensuring that human judgment is incorporated into critical decisions.
- **Engage in Continuous Learning:** Take advantage of training opportunities to develop the skills necessary for thriving in an AI-driven work environment.

Don'ts:

- **Disregard Employee Rights:** Do not use AI systems to conduct indiscriminate surveillance on employees or to manage employment relationships in an entirely automated manner.
- **Neglect Training Needs:** Avoid overlooking the importance of training and development related to AI technologies; ensure you are well-prepared for changes in the workplace.
- **Assume AI Decisions are Final:** Never treat decisions made by AI systems as final without human review; always be ready to intervene when necessary.
- **Ignore Feedback Mechanisms:** Do not dismiss employee concerns or feedback regarding AI systems; actively listen and respond to ensure a respectful workplace environment.
- **Bypass Ethical Considerations:** Avoid implementing AI solutions that could harm employee well-being or violate their rights; always consider the ethical implications of your actions.

By respecting humans and human resources in AI development and use, Median Technologies aims to create a positive impact on society, enhance employee well-being, and ensure that our AI technologies are both innovative and responsible.

9. Training and Literacy in AI Development and Use

At Median Technologies, we recognize that effective training and literacy in AI are essential for empowering our employees and ensuring the responsible use of AI technologies. This principle is vital for fostering a knowledgeable workforce that can navigate the complexities of AI while adhering to ethical standards.

9.1. Key Elements of Training and Literacy

I. **AI Literacy Programs:** We develop comprehensive AI literacy programs aimed at enhancing employees' understanding of AI technologies, ethical considerations, and responsible use. These programs are designed to equip staff with the knowledge necessary to make informed decisions regarding AI applications.

II. **Continuous Learning:** We encourage ongoing education and training to keep our employees updated on the latest trends in AI, ethical standards, and regulatory requirements. This commitment to continuous learning ensures that our workforce remains agile and adaptable in a rapidly evolving technological landscape.

III. **AI Ethics Training:** Specialized training on AI and Corporate ethics is provided to all employees, focusing on principles such as fairness, transparency, and accountability. This training ensures that everyone in the organization understands the ethical implications of their work with AI systems.

IV. **Leadership Development:** We offer advanced training for leaders on AI governance, ethics, and strategic decision-making. This empowers them to guide AI initiatives effectively and responsibly while fostering a culture of ethical AI use throughout the organization.

V. **External Collaborations:** We engage with external experts and organizations to leverage best practices in AI ethics, law compliance, and literacy. These collaborations foster a culture of continuous improvement and innovation, enhancing our training programs and ensuring they meet industry standards and statutory requirements.

VI. **Instructions for use:** We train customers and employees on how to appropriately use relevant AI systems, their capabilities, limitations, and potential risks, and give them clear guidelines on how to report errors or abuses.

9.2. Implementation of Training and Literacy Principles

Do's:

- Participate in AI Literacy Programs: Engage actively in AI literacy training programs provided by the company to enhance your understanding of AI technologies and their ethical implications.
- Commit to Continuous Learning: Stay updated on the latest trends in AI, ethical standards, and regulatory requirements through ongoing education and training opportunities.
- Complete AI Ethics Training: Attend specialized training sessions focused on AI ethics, ensuring you understand principles such as fairness, transparency, and accountability.
- Utilize Training Resources: Take advantage of resources and materials provided by the company to familiarize yourself with the capabilities, limitations, and risks associated with AI systems.
- Provide Feedback on Training: Share your insights and experiences regarding training programs to help improve their effectiveness and relevance.

Don'ts:

- Neglect Training Requirements: Do not overlook mandatory training sessions; ensure you complete all required programs related to AI literacy.
- Assume Knowledge is Sufficient: Avoid assuming that your current knowledge of AI is adequate; continuously seek to expand your understanding through available training.
- Disregard Ethical Considerations: Do not ignore the ethical implications of using AI technologies; always consider how your actions align with established ethical standards.

- Skip Documentation: Never fail to document your completion of training programs or participation in relevant workshops; this is essential for compliance verification.
- Resist Change: Do not resist new learning opportunities or changes in processes related to AI; embrace the evolving nature of technology and its implications for your work.

By prioritizing training and literacy in AI development and use, Median Technologies aims to empower its workforce, enhance ethical practices, and ensure the responsible deployment of AI technologies within the organization.

REFERENCES

- Code of Business Conduct and Ethics
- Anti-corruption / antibribery policy
- Antitrust and competition policy
- Median Technologies Risk Management Policy
- Median Technologies Data Protection Governance Model and Privacy Policy
- Median Technologies AI Usage Policy
- EU General Data Protection Regulation
- EU Artificial Intelligence Act
- EU Guidelines on Ethics in Artificial Intelligence