Medallion AI Security and Safety

Medallion's commitment to AI safety and security

At Medallion, we recognize the enormous potential of artificial intelligence (AI). We also understand that addressing AI-related risks, such as bias and security concerns, is essential to maintaining our customers' trust and confidence. To this end, we have implemented comprehensive safety and security measures across our platform. By integrating these measures, policies, and governance practices, Medallion ensures that our AI solutions meet the highest standards of security, privacy, and ethical responsibility. We remain committed to refining our practices as AI technology evolves, continuing to safeguard our clients' trust while harnessing AI's transformative potential.

AI security

We regularly audit our infrastructure and data handling processes, and we also conduct third-party security reviews on all AI models to identify and address potential vulnerabilities, ensuring compliance with strict security standards. These audits enable us to implement proactive risk management and mitigation strategies, protecting client data and maintaining system integrity. Additionally, our formal incident response plans ensure the rapid detection, investigation, and resolution of any breaches or vulnerabilities, minimizing harm and allowing for a swift restoration of operations.

Data privacy

At Medallion, we prioritize the safeguarding of client data. We strictly adhere to data privacy regulations and have robust protection measures in place. Our data management practices include encryption, access controls, and periodic audits to guard against unauthorized access and data breaches. Moreover, Medallion does not currently train models on customer data. If this changes in the future, Medallion will explicitly ask for your permission first, and participation will be strictly opt-in. All AI and machine learning capabilities within the Medallion product are held to the same stringent data privacy standards that we apply throughout our platform. This includes ensuring that any third-party provider, like OpenAI, meets our compliance requirements.

Rigorous evaluations and testing

Our AI systems go through extensive evaluations and testing to ensure their reliability and accuracy. We use a variety of testing methodologies to assess how our models perform in different scenarios. This process allows us to identify and address any issues that could affect the performance or security of our AI features.

Use of third-party model platforms

To enhance the advanced AI capabilities of the Medallion product, we leverage technology from third-party model providers, including OpenAI, Anthropic, and Reducto. Customer data is transmitted to these providers exclusively for the purposes of synthesis and generation. These model providers are not permitted to use customer data to train their models.

Human oversight

While automation is a significant benefit of AI, we believe that human oversight is essential for the ethical and responsible use of this technology. Our team regularly monitors AI outputs to ensure they meet our ethical standards and align with client expectations. This oversight helps minimize the risk of unintended consequences and enables us to make timely adjustments to our AI systems.

Continuous monitoring

We utilize continuous monitoring systems to track the performance and security of our AI features in real-time. These systems alert us to anomalies or emerging threats, enabling us to respond quickly and mitigate risks. Continuous monitoring also ensures that our AI systems remain secure and operate as intended, even as new challenges arise.

Explainability and transparency

Explainability is a priority for our AI models. Transparency allows our customers to make informed decisions and understand the limitations of AI. By fostering trust and clarity, we help our customers build confidence in our AI features and the overall performance of the platform.

Ethical AI practices

We are committed to developing and deploying AI responsibly. Our AI development process includes ethical guidelines designed to prevent biases and promote fairness. We routinely review our AI models for potential biases, taking immediate corrective actions whenever necessary. Through these ethical AI practices, we strive to provide solutions that are fair, transparent, and beneficial for all users.

If you have questions about our AI safety measures or would like to learn more about how we protect your business, please contact us at security@medallion.co.

About Medallion

Medallion is the leading provider network management platform that unites provider operations and empowers end-to-end automation workflows for credentialing, enrollment, and monitoring. We free healthcare teams to focus on what matters by enabling healthcare organizations to quickly and accurately manage and grow their provider networks with our AI-powered automation technology. By automating burdensome administration workflows, we enable operations teams to better manage their provider networks, deliver superior care, speed up revenue paths, and elevate provider satisfaction levels.

Recognized as No. 3 on Inc. Magazine's 2024 Fastest-Growing Private Companies in the Pacific Region and a Glassdoor Best Places to Work in 2024, Medallion is paving the future of provider network management. To learn more, visit Medallon.co, or join the conversation on LinkedIn.