



MHS Statement on Artificial Intelligence Use and Safeguards

At MHS, trust is foundational. We design and operate our platforms and solutions to protect sensitive information, support regulatory compliance, and preserve confidence in the outcomes we help enable.

We recognize that the use of AI raises important questions, and sometimes concerns, around privacy, security, and bias. At MHS, we are committed to addressing these responsibly by prioritizing fairness, transparency, and the highest ethical standards in everything we do.

This statement will be updated as our practices and capabilities evolve.

How is MHS currently using AI?

MHS does not currently deploy generative AI, large language models (LLMs), or agentic AI in customer-facing products, assessment delivery, scoring, or related workflows.

Our assessment platforms rely on deterministic and predictive models. Deterministic models produce consistent, reproducible outputs for a given input, while predictive models use established patterns to estimate outcomes. These models are intentionally designed to support the requirements of standardized, validated assessment in a trustful and consistent fashion.

Does MHS use customer data to train AI models?

No. MHS does not use customer assessment data, including responses, results, or personally identifiable information, to train or fine-tune generative AI models without explicit disclosure and appropriate permissions.

Where permitted by license or agreement, anonymized data may be used to enhance underlying psychometric models while maintaining deterministic, standards-aligned outputs.

How does MHS address privacy, security, and data sovereignty?

MHS designs its platforms to protect sensitive information, support regulatory compliance, and maintain strict data sovereignty aligned with its defined operational domains (MHS Corporate Operations, Janus, Portals, and Customer Integration Apps).

These controls are foundational to how MHS builds and operates its technology.

To learn more about MHS's compliance frameworks, security standards, and certifications, please visit our compliance page by scanning here.

