Artificial Intelligence

HDR acknowledges the transformative potential of artificial intelligence in our industry and communities. We embrace utilizing this technology responsibly and ethically and prioritize the client data ownership. We will always prioritize that that their data is secured by leading industry data management and data security frameworks, we protect our client and corporate data.

We adhere to the following principles to maintain standards of care and responsibility of our client's and corporate data.

- **Accountability**: We evaluate the use of artificial intelligence to ensure it is used in ways that align with our organization's values.
- **Transparency**: We promote trustworthy artificial intelligence through a commitment to transparency, providing information about our AI systems and their outputs.
- **Privacy**: Our organization recognizes privacy as a fundamental value in AI development, implementing privacy-enhancing technologies and data minimization methods to safeguard individual identity
- **Fairness**: We strive to mitigate biases and promote fairness while recognizing that this effort extends beyond demographic balance, encompassing accessibility, existing disparities, and varied cultural perceptions of fairness.
- **Fairness**: We perform assessments of generative artificial intelligence to identify and mitigate risks and perform responsible usage. We ensure AI systems meet ethical standards, and legal requirements emphasize transparent use of AI.

HDR expects all employees to act with integrity and requires all employees to follow HDR policies, including without limitation the Data Management Policy and Generative Artificial Intelligence Usage Policy.

HDR has implemented security controls and processes that comply with government and industry data protection regulations and standards. Data management controls and processes implemented at HDR include, but are not limited to, the following:

- We perform continuous oversight and reviews for AI and all software development practices to ensure compliance.
- Prohibit the use of generative AI for use in any final work product
- Clients always retain ownership of their data
- Require that written client consent for any client data use with generative AI, Opt-in vs Opt-out
- Never use client data for training or developing generative AI models
- Store and process data in accordance with client contract.
- Adhere to statutory and regulatory requirements including data sovereignty

Client data ownership

- No transfer of rights
- Right to erasure? GDPR

References: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf