Data Protection & Safety

With the rapid emergence of large language model (LLM) technology, it can be tempting to integrate these tools into everyday workflows. However, it is essential to do so in a way that safeguards both client and company data.

Risks and Considerations

Confidentiality Risks: LLMs may unintentionally retain or process sensitive data.

Compliance Requirements: Laws such as GDPR and HIPAA, along with internal policies, may restrict data sharing.

Model Limitations: LLMs can generate inaccurate, biased, or unpredictable outputs without oversight.

Best Integration Practices

Limit Sensitive Data Sharing: Avoid inputting confidential or regulated information into LLMs.

Follow Compliance Standards: Ensure all LLM use aligns with legal and organizational requirements.

Validate Outputs: Monitor and review results to catch inaccuracies or bias before use.

Ongoing Compliance

Regular Updates: Revise guidelines as laws, risks, or technology evolve.

Training & Awareness: Educate staff continuously on secure and ethical LLM use.

Feedback Mechanisms: Create channels for employees to report issues or improvements.

Accountability: Assign clear ownership for monitoring compliance and handling incidents.