COMMUNITY HEALTH CARE ASSOCIATION of New York State
chcanys.org

CHCANYS AI Vendor Vetting

Questions to Ask Vendors: How to Use This Document

This is intended to be a knowledge guide, not a checklist! Use this document to gather information and understand how well you know the technology you are using.

Introduction

When evaluating AI vendors at your center, key questions to ask should focus on data security, model transparency and bias, scalability and performance, and integration and support. It is important to ask vendors about their data handling policies, how they mitigate bias and ensure fairness, how they monitor performance, the resources required for implementation, and what support they provide for training, maintenance, and future development.

AI providers are vendors like any other and need to follow usual vetting and contracting processes for vendors. A business associate agreement (BAA) and any typical data security agreements should be completed. If possible, designate someone or multiple individuals with appropriate technology expertise, ideally in AI if available, to lead implementation and use of AI tools across your organization. This could include vendor selection, implementation, risk management, lifecycle management, compliance, and oversight.

This team could include individuals with the following expertise: executive leadership, regulatory/ethical compliance, information technology (IT), safety/incident reporting, relevant clinical/operational expertise, cybersecurity and data privacy needs, and stakeholders reflecting the needs of impacted populations (e.g., staff, providers, patients, caregivers, etc.).

Data Security and Privacy

- How is data sent to the model (e.g., prompts) secured and stored?
- How are data outputs secured and stored?
- How are data that are flagged for review (like abuses, errors) tracked and stored?
- What are your data retention and deletion policies?
- What are your data governance and ethical guidelines for data usage?
- Do you provide an AI Bill of Materials (AI-BOM) documenting all model components, training data sources, and third-party dependencies?
- What protections exist against unauthorized access or misuse?
- Do you have an ISO 42001 certification?

Model Performance and Transparency

- What type of AI model do you use, and can you explain its decision-making process?

- How do you ensure recommendations and output from the model can be explained
- What is your model's validation and verification process, and has it been clinically validated for the intended users?
- Can you provide evidence of clinical effectiveness and outcome improvements?
- What populations has the model been tested on?
- How do you monitor performance, identify, and address bias? How do you remediate?
- What are the known limitations of the system? How are you checking for new limitations, performance drift, or unexpected behaviors? How frequently is the system tested against real-world conditions?

Integration and Scalability

- How will your AI solution integrate with our existing systems?
- What resources are required for deployment and what support services do you offer?
- Can the solution be scaled to meet our future needs?

Training, Maintenance, and Support

- How, when, and for what reasons will your AI be trained and retrained over time?
- What is the process for ensuring that AI is correctly functioning after updates?
- What shutdown or rollback capabilities exist if the system malfunctions or causes harm?
- What kind of ongoing support, training, and maintenance do you provide?
- What is the plan for future development and updates?
- Is there a trial offering, or can we conduct a pilot or proof-of-concept project?

Ethics and Compliance

- What steps do you take to ensure ethical AI development and usage?
- Do you comply with NIST AI RMF trustworthiness characteristics: validity, safety, security, accountability, transparency, explainability, privacy-enhancement, and fairness?
- When AI is used in patient communications or care decisions, do you ensure disclosure to patients?
- What is the liability framework? Who bears responsibility when the AI contributes to adverse outcomes?
- How do you handle human oversight? What details can you provide about how people using your technology are kept in the loop? Is there an option to add human-review steps?

Incident Response

- What is your process for identifying and reporting AI safety incidents?
- How do you handle reported or detected model failures or unexpected behaviors?
- How will you communicate with healthcare organizations when issues arise?
- Do you conduct root cause analysis after incidents? If so, will you share those results?