



# Questions for PIAs involving AI

---

The objective of this document is to provide some basic questions about AI products and services that can be used as a basis for conducting a risk-based analysis on prospective tools, systems, and contracts.

## Preliminary questions

1. What is the name of the AI tool?
2. What is the intended outcome of using the AI tool?
3. How will the use of the AI tool enhance productivity without causing loss to existing functions and/or is recommended over more conventional tools?

## AI Questions

- 1) Is the model based on a public model, such as ChatGPT or Copilot, or is it a proprietary model using a unique codebase?
  - a. If using a public code base, does the vendor have a commercial license?
    - i. This is important because it gives an understanding of whether the institution's data will be exposed to a public model training program.
- 2) What is the source of the model training data?
  - i. This question is looking for risks around data licensing issues that could expose the institution to liability or a shut-down of operations if the model were used.
- 3) Will the institution's data train or inform the future outcomes of the model?
  - i. This question is intended to protect the institution's data and ensure that our data will not be accidentally leaked in the responses coming from the model.
- 4) Are the outcomes of the model predictable, explainable, and reproducible?
  - i. This question attempting to understand if the model is a total black box or if outcomes can be replicated. Black box algorithms can create false positives or outcomes that have hidden biases, false information, or incorrect conclusions.
- 5) How has the model been trained for fairness?
  - i. This question is looking specifically at bias and whether the algorithm creators have examined the outputs for hidden or blatant biases, particularly on protected grounds of discrimination.
- 6) Has the algorithm undergone, and does it continue to undergo, adversarial testing?
  - i. This question is looking at whether the algorithm has been tested to see if it can be forced to behave in an unintended way.
- 7) What is the process for review and correction of the algorithm?
  - i. This question is looking at algorithmic drift and ensuring the model continues to operate in as accurate and complete a manner as intended.