Summary of Flatiron's Predictive DSI Intervention Risk Management Practices

At this time, Flatiron does not internally develop any predictive DSI ("pDSI") functionality; however, it does collect all required risk analysis, risk management, and governance documentation from externally developed pDSI functionality that is supplied by Flatiron as part of its Certified Health IT product, OncoEMR® (see Vendor Questionnaire in Appendix 1).

For any externally developed pDSI we choose to supply, Flatiron requires the developer (hereafter, "developer" and "vendor" are used interchangeably to refer to the external party supplying the pDSI functionality) to provide information regarding how it analyzes, mitigates, and resolves risk associated with the intervention on the following dimensions:

- Validity
- Reliability
- Robustness
- Fairness
- Intelligibility
- Safety
- Security
- Privacy

Flatiron assesses the developer's responses to ensure standards are met according to Flatiron's Quality Management System (QMS). If a given developer's responses do not meet Flatiron's standards, we will work with the vendor to reach a mutually agreeable risk mitigation strategy such that the intervention meets Flatiron standards. Only vendors who provide satisfactory responses regarding their risk analysis, risk mitigation, and governance practices will be deployed in OncoEMR.

Additionally, Flatiron's QMS ensures that throughout the software development lifecycle, externally developed pDSI are integrated in a manner that centers quality and usability and are carefully deployed with appropriate testing. Flatiron conducts its own Safety Enhanced Design (SED) testing for pDSI functionality to ensure it is safely deployed within OncoEMR.

Risk Analysis

All pDSIs at Flatiron are subject to a risk analysis process to identify and assess potential risks and adverse impacts associated with the following characteristics: validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy.

Flatiron rigorously vets all "Supplied by" pDSI options among these domains and ensures only the most robust solutions are selected for integration. For vendors that we partner with to

supply pDSI in OncoEMR, we gather information on how they identify and assess potential risks and adverse impacts in their development of AI algorithms used in patient care.

If any gaps or concerns are identified during review, Flatiron collaborates with the vendor to address them prior to deployment.

Risk Mitigation

Identified risks are addressed through a combination of design controls, process controls, and user-facing informational controls to ensure that risks are reduced to acceptable levels prior to release. Flatiron requires vendors to document specific mitigation strategies. These may include:

- Design Controls: Implementation of technical safeguards or workflow modifications to reduce risk.
- Informational Controls: Clear communication to users about known risks and recommended actions.
- Testing and Validation: Requirement for vendors to conduct and document quality assurance testing, including pilot deployments with real-world data where feasible.
- Incident Response: Documentation of processes for identifying, reporting, and resolving issues post-deployment, including escalation paths for safety-related incidents.

Flatiron reviews all vendor-provided mitigation strategies as part of its QMS. If mitigation is insufficient, Flatiron works with the vendor to develop additional controls or may choose not to deploy the pDSI. Flatiron also conducts its own SED testing prior to deployment to ensure that pDSIs are safely deployed within OncoEMR. Ongoing monitoring and incident management processes are in place to address any issues that arise after deployment.

Governance

Flatiron maintains robust AI governance policies and controls for all pDSIs, including a protocol specific to vendors. Vendors must provide evidence of effective internal governance practices, including oversight mechanisms, policies, and independent review processes for the development and deployment of their algorithms. Accepted examples include:

- Internal oversight structures for pDSI development and deployment, including pre-release and regular audits of model output for clinical relevance, correctness, and safety.
- Data acquisition, management, and use policies with data quality controls to reduce bias and ensure fairness.
- Transparency measures such as user documentation, release notes, communication of known limitations or risks, and clear escalation paths for high-severity issues.

Only vendors with satisfactory governance practices are approved for integration into OncoEMR. Management reviews are in place to ensure that externally developed pDSI are deployed in accordance Flatiron's QMS standards.

Appendix

Appendix 1: Vendor Questionnaire

Questions for “Supplied By” Vendor

As a certified health IT developer, Flatiron has certain obligations with regard to risk management for AI-enabled functionality deployed in EHR. For vendors that we work closely with to deploy their technology in our product, we need to collect information on how they manage risk in their development of AI algorithms used in patient care. Please respond to the following questions and address how you will assess, mitigate, and resolve various aspects of risk that may be associated with your model to provide assurances that your company’s intervention risk management policies meet ONC standards under (b)(11). Include your procedures and internal steps for anticipating and preventing undue risk, the review frequency and resolution timelines when risks or notable issues are determined, and how changes to address identified risks are tested, communicated and deployed - including partner communication. We do not require you to provide any information that puts your IP or trade secrets at risk, but would be happy to discuss signing an NDA if that makes you more comfortable.

Question	Answer
How does your organization approach governance for the development and deployment of predictive algorithms? Specifically, what oversight mechanisms, policies, and independent review processes are in place to oversee and ensure the deployment of the algorithms included in your product?	
How do you assess, mitigate, and resolve any risks associated with the validity of the trained algorithms included in your product?	
How do you assess, mitigate, and resolve any risks associated with the reliability of the trained algorithms included in your product?	
How do you assess, mitigate, and resolve any risks associated with the robustness of the trained algorithms included in your product?	

How do you assess, mitigate, and resolve any risks associated with the fairness of the trained algorithms included in your product?	
How do you assess, mitigate, and resolve any risks associated with the intelligibility of the trained algorithms included in your product?	
How do you assess, mitigate, and resolve any risks associated with the safety of the trained algorithms included in your product?	
How do you assess, mitigate, and resolve any risks associated with the privacy and security of the trained algorithms included in your product?	