Plan – Intervention Risk Management – Predictive DSI

Author	David Walker	**Created**	9/14/2025
Document	COMP-05-0002	**Approval**	9/24/2025
Version	1	**Effective**	10/1/2025
Review	Annual	**Updated**	N/A
Classification	Confidential		
Controls	164.308(a)(1), 164.502(b), 164.308(b)(1), 164.514, 164.312(b), CC3.1-3.4, CC9.1, PI1.1-1.5, P3.1-3.2, P4.1, CC6.6, CC9.2, CC4.1, C1.1-1.2		

Table of Contents

Classification

Scope

This Summary applies to Predictive DSI functionality supplied by Intellicure in its certified EHR software.

Purpose

This summary outlines the steps and controls that Intellicure has implemented to ensure the responsible development, deployment, and use of certain AI-powered features within our Electronic Health Record (EHR) system and associated components. This document contains a summary of risk management activities performed by Intellicure for each of its Predictive Decision Support Interventions (DSI) in compliance with the ONC Health IT Certification Program.

A Predictive DSI is defined as technology that supports decision making based on algorithms or models that derive relationships from training data and then produces an output that results in prediction, classification, recommendation, evaluation, or analysis. These features can help leverage data and predictive analytics to aid healthcare decision-making.

Intellicure's commitment to safety, privacy, transparency, and preventing bias remains at the forefront as we integrate AI technology into our products.

Terms

The following table lists the terms used in this document:

Term	Definition
Predictive Decision Support Intervention (Predictive DSI)	Defined by the ASTP/ONC as technology that supports decision making based on algorithms or models that derive relationships from training data and then produce an output that results in prediction, classification, recommendation, evaluation, or analysis. Note that not all AI features created by Intellicure are considered Predictive DSI.

Intervention Risk Management Plan

The following risk management activities are performed as part of Intellicure's risk management processes and governed by Intellicure's Quality Management System.

Process Overview

When Intellicure determines that an AI feature it offers meets the definition of a Predictive DSI, the detailed functionality of the Predictive DSI is documented in the form of design input requirements and analyzed to identify risks, including those posed to the validity, reliability, robustness, fairness,

intelligibility, safety, security, and privacy of the output. Each Predictive DSI is subject to commensurate risk analysis and mitigation activities as outlined below.

Risk Analysis

Predictive DSI are subject to analysis of potential risks and adverse impacts in accordance with Intellicure's Quality Management System. Analysis includes risks related to the Fairness, Appropriateness, Validity, Effectiveness, Safety, Security, and Privacy of the intervention.

Intelligibility

Product features are reviewed by software usability and human-machine-interface experts to ensure that users of the Predictive DSI are aware that the intervention output has been generated by predictive models and understand how to take any actions that may be necessary to confirm the outputs before acting on them.

Security

Product features are reviewed for security risks by cybersecurity experts with experience in evaluating machine learning and predictive models. These reviews include testing for common attacks such as prompt injection, data leakage, and insecure output handling, among others.

Reliability and Robustness

Prior to being made available for general use, the Predictive DSI is piloted with select healthcare providers to provide a practical environment to test the performance of the intervention against actual patient data and clinical workflows (if applicable). This testing evaluates the impact of the intervention on patient outcomes and operational efficiencies to ensure the intervention is performing its intended function reliably. These pilots also present the intervention with unique challenges and edge cases that may not be captured in the controlled data set used to test them in development. Identifying these scenarios allows for the identification of risks and limitations that were not foreseen in the initial risk analyses and ensures the system is robust enough to operate successfully in varied environments.

Fairness

Inputs to Predictive DSI are limited to only that information which is necessary for the intervention to function. To significantly mitigate risk of bias in the intervention, demographic characteristics which are not necessary for the intervention are not provided to the system.

When necessary and commensurate with the risk of the intervention, additional bias testing in the form of demographic parity testing is performed to determine if the intervention produces outputs for a demographic that are substantively different from the outputs of the general population and evaluate if those differences reflect a legitimate difference in the population.

Privacy

Predictive DSI are developed under defined contractual relationships with third party software providers. These contracts stipulate that data inputs and outputs will not be used by the third party to train or develop additional predictive models and will not be recorded or retained by the third party. In the event a Predictive DSI utilizes training or testing data, real-world de-identified customer data was used as the source, as documented in the source attributes available for review in the software. These contracts are established in addition to any Business Associate Agreements and privacy policies required by HIPAA and other applicable legislation.

Validity and Safety

Predictive DSI is classified as either clinical or non-clinical. A clinical intervention is one that has the potential to impact a provider's medical decision-making and could potentially impact the patient's care or the patient's medical record.

Non-clinical Predictive DSI are reviewed by the Product Management and Quality Assurance teams during their validation step in the software development life cycle.

In addition to Product Management and Quality Assurance review, clinical Predictive DSI are reviewed by licensed clinicians who possess the clinical knowledge and practical experience necessary to assess the validity of intervention outputs within real-world healthcare settings. Their involvement in the review process ensures that the intervention outputs are relevant to current clinical practices and align with established medical guidelines. These clinicians are trained to identify potential safety risks associated with decision support tools and their integration within EHR software. Their reviews conform to standards for managing clinical risks in health IT software and help ensure that safety and validity risks are mitigated prior to the release of the intervention. Specifically, the levels of review and applied to clinical Predictive DSI are included in the table below.

The following clinical risk assessment methodology is applied to each clinical Predictive DSI:

Clinical Review	A Predictive DSI undergoes clinical review of its Design Input Requirements to assess risk and identify and document risk reducing controls in the module or feature.
Module Categorization	Each Predictive DSI is part of a module that is categorized based on a combination of the impact to the patient or public health and the healthcare situation or condition. Risk analysis activities are performed commensurate with the categorization of the module.
Hazard Log	A hazard log is created to document all hazards, causes and controls associated with the applicable module or feature. Initial risk (severity or likelihood and risk level) and residual risk (considering risk reducing controls) are both documented. The hazard log serves to map user stories housed within the Design Input Requirements to the design controls in place to ensure the feature effectively reduces clinical risk.
Clinical Validation	Clinicians evaluate the clinical output of the Predictive DSI to determine if the output meets clinical quality and safety expectations. This analysis is performed by the Medical Team clinicians and in certain situations in conjunction with external vendors.
Quality Assurance Testing	Each Predictive DSI undergoes quality assurance testing according to internal policies and in conformance with international software development standards.

Risk Mitigation

Where risk analysis activities identify a risk in a Predictive DSI, controls are created to mitigate the risk to an acceptable level. These risk controls take the form of additional design requirements that are added to the design input requirements to eliminate or mitigate the intervention's ability to produce the risk. Where it is not possible to eliminate the risk through product design,

informational controls are added to inform the intervention user of the risk and direct them to take appropriate actions outside of the intervention to prevent the potential harmful effect of the risk from being realized.

Each risk control requirement is given a unique identifier and mapped to all quality assurance activities which verify its effectiveness and correct functioning. The test protocols, the identity of the person responsible for executing the test, and the results of each execution of the test are recorded and the records maintained for the lifetime of the product.

Governance

All activities described as part of this intervention risk management plan or otherwise involved in the design, development, and maintenance of Predictive DSI are subject to the governance of the Quality Management System and Software Development Lifecycle Policy. For example, this includes how source attribute data are acquired, managed and used in the system.

Related Standards, Policies, and Procedures

Applicable Public Standards

- NIST Secure Software Development Framework (SSDF)

Applicable Standards from the SOC 2 Trusted Services Criteria

- CC3.1-3.4 – Risk Assessment
- CC9.1 – Risk Mitigation
- PI1.1-1.5 – Processing Integrity
- P3.1-3.2, P4.1 – Privacy Collection and Use
- CC6.6 – Security Measures
- CC9.2 – Vendor Management
- CC4.1 – Ongoing Evaluations
- C1.1-1.2 – Confidentiality

Applicable Standards from the HIPAA Security Rule

- §164.308(a)(1) – Risk Analysis and Risk Management
- §164.502(b) – Minimum Necessary
- §164.308(b)(1) – Business Associate Agreements
- §164.514 – De-identification
- §164.312(b) – Audit Controls

Related Intellicure Documents

- DEV-01-0002 – Policy – AI-ML
- CORP-01-0010 – Risk Analysis of ePHI
- ITS-01-0002 – De-Identification
- CORP-01-0014 – Business Associates

Version History

Version	Date	Summary
1	9/14/2025	Original document.

Document Review

Date	Type	Reviewer
9/14/2025	Original	David Walker