

Background

Artificial Intelligence (AI) systems are now integral to clinical research processes, such as automated adverse event detection in clinical trials, patient eligibility screening for protocol enrollment & data quality validation but may create safety, accountability, and compliance risks.

Problem

Problem Statement: A high-profile **example** is the Epic Sepsis Model, a proprietary algorithm deployed in numerous hospitals, which failed to identify **67% of patients with sepsis** while generating alerts for only 18% of admissions.

Objectives

While each framework emphasizes critical aspects of trustworthy AI, This SMART+ Framework introduces a streamlined taxonomy tailored for Clinical Research. It integrates the core principles of Safe, Monitored, Accountable, Reliable, and Transparent (SMART), augmented with Privacy & Security, Data Governance, Fairness & Bias, and Guardrails.

Safe

Ensures the AI system operates without causing harm to individuals or society.

Monitored

Continuously observes system performance, safety, and ethical compliance.

Accountable

Guarantees that human roles and responsibilities for AI outcomes are clearly defined.

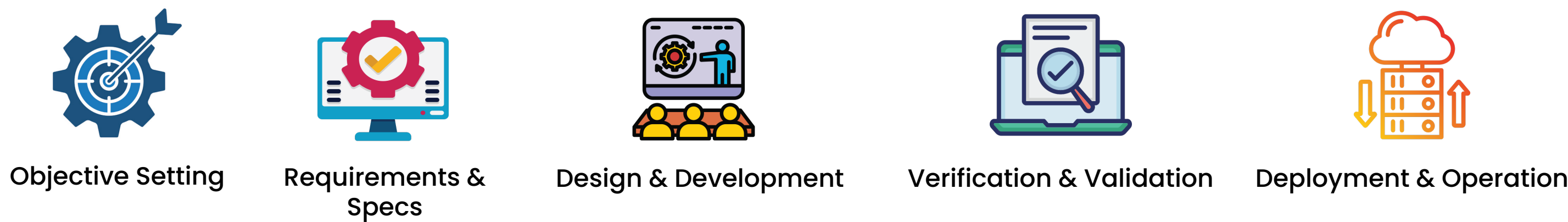
Reliable

Performs consistently, accurately, and predictably across different conditions.

Transparent

Makes the AI's decision-making processes understandable to relevant stakeholders.

Integrated Across the Full AI Lifecycle



A Risk-Stratified Approach

Governance intensity scales to match the system's risk level (Low, Medium, or High).



Principles are embedded in every stage, from objective setting to long-term operation.

Example: SDTM Data Conversion

Risk Assessment – SDTM Data Conversion

- Model influence – Medium (Model Contributes Meaningfully)
- Decision Consequence – Medium (Influence interpretation based on severity, probability and detectability)
- Risk-Medium

Pillar	Parameters	Evidence
Safety	Intended purpose and SDTM data conversion boundaries defined (e.g., domains covered, no clinical decision-making) Preliminary safety and data integrity risk assessment completed for SDTM mapping and transformation	Reviewed SDTM Conversion Specification and scope statement Verified Risk Assessment FMEA scenarios covering mapping errors, data loss, traceability risks
Monitored	Monitoring plan defined for SDTM data conversion quality (KPIs, frequency, roles)	Approved Monitoring Plan including % mapping errors, rejected records, reconciliation rates
Accountability	Key roles and responsibilities for SDTM conversion defined (Data Standards, Clinical Programmer, Programming Lead, QA)	Reviewed RACI matrix
Reliability	SDTM conversion accuracy and consistency objectives defined, tested, and verified	Reviewed SDTM verification and reconciliation report (source vs SDTM)

Pillar	Parameters	Evidence
Transparency	SDTM mapping logic, derivation rules, and assumptions documented and traceable	Reviewed SDTM Mapping Specification and Requirements Specification
Privacy / Security	Privacy and security risks assessed for subject-level clinical data during SDTM data conversion	Confirmed approved Data Protection Impact Assessment (DPIA) and security risk assessment reports
Data Governance	Source datasets, controlled terminology, and SDTM standards versions identified and approved	Reviewed data inventory, CDISC version approvals, and change control records
Fairness / Bias	Bias risk assessed related to data transformations or subgroup handling in SDTM derivations	Reviewed fairness and data integrity risk assessment report
Guardrails	Guardrails defined and verified to prevent out-of-scope or invalid SDTM transformations	Reviewed guardrail verification report (e.g., domain checks, controlled terminology validation, reject rules)

Outcome: Controlled, auditable, and GxP-compliant process, fully consistent with SMART+ principles and regulatory expectations.

Key Takeaways

