## Claims

1. **A hospital-wide sentinel-event automation and reporting system**, comprising: a plurality of **device and software connectors** configured to receive heterogeneous event data from medical devices and clinical information systems throughout a healthcare facility; a **normalization module** that transforms incoming event data into a unified schema; a **priority-based triage engine** that assigns a risk severity and urgency score to each normalized event; a **rules engine** encoding state regulatory thresholds and Patient Safety Quality Improvement Act (PSQIA) guidelines, the rules engine determining required reporting actions for each event based on event attributes and said encoded thresholds; an **export engine** that automatically formats and transmits event reports to external systems and authorities as determined by the rules engine; and an **immutable ledger module** that records each event and processing step in a tamper-evident log, **wherein** the system is operable to federate sentinel events from multiple sources into a central registry and autonomously route each event through triage, compliance decision, and reporting workflows.

2. **The system of claim 1**, wherein the plurality of device connectors includes prebuilt adapters for smart infusion pumps, electronic health record medication administration modules, surgical site tracking systems, fall detection sensors, implantable device monitors, and behavioral health risk assessment tools, each connector being configured to capture and transmit sentinel-event data from its respective source in real-time into the normalization module.

3. **The system of claim 1**, wherein the priority-based triage engine calculates a **priority score** for each event as a function of the event's harm severity and time-to-harm urgency, and categorizes events into priority levels such that high-severity, imminent-risk events are flagged for immediate attention and escalated response.

4. **The system of claim 1**, wherein the rules engine comprises a knowledge base of **jurisdiction-specific sentinel event definitions and reporting criteria**, and wherein the rules engine automatically compares each event's characteristics to said criteria to determine if the event is mandatorily reportable to a state authority, reportable to an accrediting body, eligible for confidential submission to a Patient Safety Organization (PSO) under PSQIA safe harbor, or any combination thereof.

5. **The system of claim 1**, wherein the export engine includes: a **state reporting module** that populates event information into state-required incident report formats or electronic portals; a **PSO submission module** that packages event data according to standardized patient safety event formats[2] for transmission to a PSO's database; and an **internal integration module** that creates or updates incident records in internal risk management and root-cause analysis systems, thereby distributing the event data to all relevant external and internal recipients without manual data re-entry[8].

6. **The system of claim 1**, wherein the immutable ledger module uses cryptographic hashing and sequential linking of records such that each event entry and its subsequent

processing actions form an immutable audit chain, providing a transparent and tamper-proof timeline of the sentinel event's detection, analysis, and reporting[9].

7. **The system of claim 1**, further comprising a **clinician override interface** that allows authorized personnel to review and modify the system-suggested classification or reporting actions for an event prior to external submission, **wherein** any such override decision and associated user input are logged by the ledger module as additional entries linked to the original event, thereby preserving an audit trail of human interventions in the automated process.

8. **The system of claim 1**, wherein the system is interoperable with external healthcare IT platforms via standard protocols such that: sentinel events can be annotated with data pulled from an electronic health record (EHR) system (including patient demographics and clinical context), and incident records or alerts can be pushed into third-party systems including EHR notification feeds, automated medication dispensing cabinet logs, or enterprise incident management software (RLDatix or equivalent), enabling cross-platform continuity of the event information.

9. **The system of claim 1**, wherein the normalization module and rules engine are configured to be extensible to new event types and sources by updating schema definitions and rule sets, respectively, allowing the addition of **new sentinel-event categories** (including but not limited to radiological errors, laboratory diagnostic errors, or health IT system failures) without architectural modification to the system, thereby supporting modular expansion to non-infusion and emerging sentinel events.

10. **The system of claim 1**, wherein the system provides real-time notification to clinical and administrative users upon detection of a high-priority sentinel event, and tracks acknowledgment of such notifications, **such that** if a triggered alert is not acknowledged within a preset time, the system escalates the alert to additional personnel or layers of management, ensuring critical events elicit timely human response in parallel with the automated reporting process.