Utility Patent Application

Patent Title

WM-001, WM-003, and WM-005 Integrated 8-Bed Ward Enterprise IT Implementation (WD-Series) with HSA Class B Software as a Medical Device (SaMD) and FDA Verification and Validation Protocols for Eldercare Constitutional Governance.

Application Information

Application Type: Utility Patent (Non-Provisional)

Nice Classification: Classes 10, 44, and 45

Field of Regulatory Scope: Health Sciences Authority (HSA) Class B Software as a Medical Device (SaMD); U.S. Food and Drug Administration (FDA) Software as a Medical Device Verification and Validation

Technology Domain: Eldercare Constitutional Governance, Artificial Intelligence-Driven Medical Software, Biosensing and Monitoring Systems, Enterprise IT Clinical Integration, LiDAR-Based Fall Prevention, Iris Biometric Authentication, Ambient Care Intelligence

Inventors

Edwin Koh Wui Kiat

Date: 6th May 2026.

Assignee

Edwin Koh Wui Kiat

Priority Data

[Priority Application Number and Date to be inserted]

Field of the Invention

[0001] The present invention relates to an enterprise-grade, constitutionally governed clinical integration system for eldercare ward environments, and more particularly to the integrated deployment of WM-Series medical hardware devices — comprising the WM-001 vital sign monitor, the WM-003 fall prevention LiDAR and thermal sensing system, and the WM-005 diagnostic iris and eye scanner — within an **8**-bed eldercare ward governed by WD-Series constitutional software protocols, including WD115 Ambient Care Intelligence, WD116 Silent Elder Protocols, WD071 Eldercare Drift

Correction, and WD117 Compliance Framework. The invention is directed to achieving HSA Class B Software as a Medical Device (SaMD) regulatory approval and FDA Verification and Validation (V&V) protocol compliance through a unified, constitutionally enforced, cryptographically immutable governance architecture.

[0002] The invention encompasses constitutional governance architectures for sensing, monitoring, and controlling devices operating under Nice Classification Classes 10, 44, and 45, wherein the WD-Series framework enforces regulatory compliance, ethical governance, algorithmic accountability, patient dignity preservation, and patient safety constraints through a hierarchically structured constitutional layer embedded within the SaMD operational architecture of each WM-Series device and their collective integration within the ward-level enterprise IT environment.

Background of the Invention

[0003] The proliferation of intelligent medical hardware in eldercare ward environments has created complex regulatory, ethical, and operational challenges. Eldercare inpatient wards operating with multiple co-located patients — each presenting heterogeneous physiological, cognitive, and legal profiles — require integrated monitoring and intervention systems that simultaneously preserve patient dignity, ensure clinical safety, satisfy regulatory mandates, and maintain comprehensive audit traceability.

[0004] Existing ward-level monitoring deployments typically integrate vital sign monitors, fall detection systems, and diagnostic devices as operationally siloed hardware units without a unifying constitutional governance layer. Current systems fail to address the regulatory requirement for a Software as a Medical Device governance architecture that systematically enforces ethical constraints, privacy preservation, surrogate consent management, and AI behavioral accountability at the ward level.

[0005] The Health Sciences Authority (HSA) of Singapore under its Regulatory Framework for Software as a Medical Device, and the U.S. Food and Drug Administration (FDA) under its Software as a Medical Device Guidance documents, require that Class B SaMD products demonstrate clinical evidence of safety and effectiveness, risk management in compliance with ISO 14971, and quality management systems aligned with ISO 13485. No prior art discloses a ward-level constitutional framework that embeds enforceable WD-Series governance protocols directly into the computational architecture of co-deployed WM-Series medical hardware devices as a unified structural regulatory compliance mechanism.

[0006] Eldercare wards present unique challenges that compound these regulatory deficiencies. Elderly inpatients in multi-bed ward configurations are frequently unable to provide real-time informed consent due to cognitive impairment, dementia, or reduced decisional capacity. Autonomous AI-driven sensing, monitoring, and controlling devices operating in shared ward spaces require constitutional governance layers that preserve patient autonomy, prevent cross-patient data contamination, ensure algorithmic transparency, and enforce structured escalation pathways for unauthorized AI authority expansion — a condition herein designated as Constitutional Drift.

[0007] Furthermore, no prior art discloses a ward-level implementation wherein LiDAR point-cloud and thermal matrix sensing data are constitutionally classified as Ambient Care Intelligence, wherein iris biometric authentication governs clinician-level access to sensitive diagnostic outputs, wherein hardware interrupts are triggered by Drift Correction protocols at the ward enterprise IT layer, and wherein all constitutional enforcement events are recorded in a cryptographically immutable distributed ledger satisfying both HSA and FDA regulatory submission requirements.

[0008] There exists a long-felt but unmet need in the art for a constitutionally governed, enterprise IT-integrated, multi-device eldercare ward implementation that is simultaneously HSA Class B SaMD compliant, FDA V&V compliant, ethically sound, technically implementable, and operationally complete across sensing, monitoring, and controlling SaMD subsystems operating in an 8-bed eldercare ward environment.

Summary of the Invention

[0009] The present invention provides a WD-Series Constitutionally Governed Enterprise IT Integration Architecture for WM-Series Medical Hardware in an 8-Bed Eldercare Ward, hereinafter referred to as the "WD-WM Ward Integration System" or the "System," comprising a hierarchically structured constitutional governance architecture embedded within and across the WM-001, WM-003, and WM-005 medical hardware devices and their supporting enterprise IT infrastructure, governed by the WD115, WD116, WD071, and WD117 constitutional software protocols.

[0010] In one aspect, the invention provides a WD115 Ambient Care Intelligence module configured to classify all WM-001 vital sign monitoring outputs and all WM-003 LiDAR point-cloud and thermal matrix sensing outputs as passive, non-identifiable, clinically purposeful Ambient Care Intelligence data streams, enforcing constitutional privacy preservation constraints that ensure the dignity of every patient within the 8-bed ward environment.

[0011] In another aspect, the invention provides a WD116 Silent Elder Protocols module configured to activate a Zero-Default Harm Principle for all patients determined by a cognitive status assessment engine to lack decisional capacity, and to enforce Proxy Constitutional Appointments for surrogate consent management, wherein the WM-005 iris biometric authentication system gates all authorized clinician access to sensitive diagnostic data outputs.

[0012] In a further aspect, the invention provides a WD071 Eldercare Drift Correction module configured to continuously monitor WM-Series device operational behavior for Constitutional Drift — defined as unauthorized AI authority expansion beyond constitutionally permissible operational envelopes — and to trigger hardware interrupts or Tier 2 escalation procedures upon detection of drift events, ensuring constitutional supremacy is maintained at all operational levels.

[0013] In yet a further aspect, the invention provides a WD117 Compliance Framework module configured to record all constitutional enforcement events, Sacred Pause delays, drift flags, biometric unlock events, and compliance attestations in a cryptographically immutable distributed ledger, generating structured regulatory submission data packages satisfying ISO 14971 risk management requirements, ISO 13485 quality management requirements, and IEC 62304 medical device software

lifecycle requirements for HSA Class B SaMD Pre-Market Submission and FDA V&V protocol compliance.

[0014] The WD-WM Ward Integration System achieves technical advantages including enhanced ward-level regulatory traceability, reduced risk of AI-induced patient harm, improved cross-device clinical transparency, systematic alignment with HSA and FDA SaMD regulatory requirements, and constitutional enforcement of patient dignity and safety constraints across all 8 patient care stations within the ward enterprise IT environment.

Brief Description of the Figures

[0015] The accompanying figures, which are incorporated in and constitute a part of this specification, illustrate embodiments of the invention and together with the description serve to explain the principles of the invention.

[0016] **FIG. 1** is a high-level architectural block diagram of the WD-WM Ward Integration System illustrating the 8-bed ward topology, WM-Series device deployment positions, WD-Series protocol governance layers, enterprise IT integration backbone, and constitutional enforcement pathways across sensing, monitoring, and controlling subsystems.

[0017] **FIG. 2** is a flowchart illustrating the integrated ward-level constitutional compliance verification workflow, beginning with WM-003 detection events, proceeding through WD115 Ambient Care Intelligence privacy validation, WD071 Drift Correction verification, Sacred Pause clinician verification via WM-005 iris biometric authentication, and culminating in WD117 immutable ledger recording for regulatory audit.

[0018] **FIG. 3** is a schematic diagram of the WM-001 vital sign monitor subsystem illustrating the constitutional vital data acquisition controller, physiological sensor arrays, privacy-preserving signal processing pipeline, WD115 ambient classification engine, and WD116 Zero-Default Harm enforcement module as integrated within the 8-bed ward environment.

[0019] **FIG. 4** is a block diagram of the WM-003 fall prevention LiDAR and thermal sensing subsystem illustrating the multi-beam laser emitter array, time-of-flight engine, point-cloud generation module, thermal matrix processor, WD115 ambient classification gate, WD071 drift monitoring interface, Sacred Pause trigger logic, and sovereignty gate governing sensor output release.

[0020] **FIG. 5** is a schematic diagram of the WM-005 diagnostic iris and eye scanner subsystem illustrating the iris biometric authentication engine, WD116 clinician authorization gateway, diagnostic output controller, constitutional inference validation unit, and WD117 biometric unlock event recorder.

[0021] **FIG. 6** is a data flow diagram of the WD117 Compliance Framework distributed ledger architecture illustrating cryptographic immutability mechanisms, constitutional enforcement event recording, Sacred Pause delay timestamping, drift flag inscription, biometric unlock logging, compliance attestation storage, and regulatory submission data packaging for HSA Pre-Market Submission and FDA V&V protocol evidence.

[0022] **FIG. 7** is a process flow diagram of the WD071 Eldercare Drift Correction module illustrating Constitutional Drift detection logic, hardware interrupt generation pathways, Tier 2 escalation protocols, drift flag recording, and constitutional restoration procedures for WM-Series device governance.

[0023] **FIG. 8** is a schematic diagram of the WD116 Silent Elder Protocols module illustrating the Zero-Default Harm Principle enforcement engine, cognitive status assessment module, Proxy Constitutional Appointment registry, tiered consent authorization protocol, and WM-005 iris biometric authentication integration for clinician access gating.

[0024] **FIG. 9** is a diagram of the HSA Class B SaMD and FDA V&V Regulatory Alignment Matrix, mapping each WD-Series constitutional protocol to corresponding HSA regulatory requirements, FDA SaMD guidance provisions, ISO 14971 risk control elements, ISO 13485 quality management elements, and IEC 62304 software lifecycle requirements.

Detailed Description of the Preferred Embodiments

I. Overview of the WD-WM Ward Integration System

[0025] Referring now to FIG. 1, the WD-WM Ward Integration System 100 comprises a constitutionally governed enterprise IT integration architecture operatively coupling the WM-001 vital sign monitor 110, the WM-003 fall prevention LiDAR and thermal sensing system 120, and the WM-005 diagnostic iris and eye scanner 130 across an 8-bed eldercare ward topology 140. The System 100 is governed by four WD-Series constitutional software protocol modules: the WD115 Ambient Care Intelligence module 150, the WD116 Silent Elder Protocols module 160, the WD071 Eldercare Drift Correction module 170, and the WD117 Compliance Framework module 180.

[0026] The enterprise IT integration backbone 190 operatively couples all WM-Series hardware devices to the WD-Series protocol governance layers, providing a unified constitutional enforcement architecture that governs all sensing, monitoring, and controlling operations within the 8-bed ward environment. The constitutional enforcement architecture is hierarchically ordered such that patient safety and dignity provisions supersede operational efficiency provisions at every layer of the System 100.

[0027] In a preferred embodiment, each of the **8** patient care stations within the ward 140 is equipped with a constitutionally governed instance of each WM-Series device, collectively forming a ward-level sensor fusion environment in which physiological monitoring, fall detection, and diagnostic scanning operations are simultaneously governed by the WD-Series constitutional protocol stack. The enterprise IT integration backbone 190 maintains constitutional enforcement across all patient care stations, ensuring that no device output is transmitted, acted upon, or logged without prior constitutional validation by the relevant WD-Series protocol module.

II. WD115 Ambient Care Intelligence Module

[0028] Referring now to FIG. 3 and FIG. 4, the WD115 Ambient Care Intelligence module 150 governs the constitutional classification of all WM-001 and WM-003

operational outputs within the 8-bed ward environment. The module 150 enforces a constitutional classification standard that designates all LiDAR point-cloud vector data streams, thermal matrix data streams, and physiological monitoring data streams as Ambient Care Intelligence, defined as passive, non-identifiable, clinically purposeful data representations that preserve patient dignity by precluding individual biometric identification from sensor outputs in the absence of explicit constitutional authorization.

[0029] Constitutional Article WD115.1 provides that all WM-003 point-cloud vectors and thermal matrices shall be processed through the WD115 Ambient Classification Engine 152 prior to any downstream clinical inference operations, ensuring that raw sensor data is constitutionally transformed into dignity-preserving Ambient Care Intelligence representations. Constitutional Article WD115.2 provides that no WM-001 physiological data stream shall be transmitted beyond the constitutional data governance boundary without a WD115 ambient classification attestation record. Constitutional Article WD115.3 provides that the WD115 module shall enforce constitutional data minimization constraints, limiting sensor data retention to the minimum clinically necessary for the declared clinical purpose of fall prevention and vital monitoring.

[0030] In a preferred embodiment, the WM-003 LiDAR subsystem 120 generates point-cloud vector representations of the ward spatial environment at a constitutional sensing refresh rate. The point-cloud vectors are classified by the WD115 Ambient Classification Engine 152 as non-identifiable spatial representations when no fall event, gait anomaly, or high-risk posture is detected. Upon detection of a constitutional trigger condition — including a fall event, a high-risk posture exceeding constitutional threshold parameters, or a bed-exit detection event — the WD115 module 150 initiates the constitutional compliance verification workflow depicted in FIG. 2.

[0031] The WD115 thermal matrix processing pipeline 154 governs the classification of WM-003 thermal sensor outputs, applying constitutional thermal anonymization protocols that prevent individual patient identification from thermal imaging data while preserving the clinical utility of thermal gradient analysis for fall risk assessment and patient position monitoring.

III. WD116 Silent Elder Protocols Module

[0032] Referring now to FIG. 8, the WD116 Silent Elder Protocols module 160 governs the constitutional management of patient care operations in the 8-bed ward for patients determined to lack decisional capacity. The module 160 activates the Zero-Default Harm Principle 162, which mandates that all WM-Series device operations defaulting to clinical action in the absence of explicit patient consent shall be constitutionally validated against the precautionary harm prevention standard before execution.

[0033] Constitutional Article WD116.1 provides that upon determination by the Cognitive Status Assessment Module 164 that a patient lacks decisional capacity, the WD116 module 160 shall immediately activate Zero-Default Harm Principle enforcement for all WM-Series device outputs pertaining to that patient, suspending all non-essential clinical recommendation outputs pending Proxy Constitutional Appointment authorization. Constitutional Article WD116.2 provides that the Proxy

Constitutional Appointment Registry 166 shall maintain records of all legally authorized surrogate decision-makers for each registered ward patient, including legal guardians, lasting power of attorney holders, and designated healthcare representatives, and that all clinical actions requiring patient consent shall be authorized by a constitutionally valid Proxy Constitutional Appointment record before execution.

[0034] Constitutional Article WD116.3 provides that all authorized clinician access to WM-005 diagnostic iris and eye scanner outputs for cognitively impaired patients shall be authenticated through the WM-005 iris biometric authentication engine 132, ensuring that sensitive diagnostic data is released only to constitutionally authorized clinical personnel. The WM-005 iris biometric authentication engine 132 implements a constitutional biometric authorization protocol comprising iris scan acquisition, biometric template matching against the authorized clinician registry, constitutional authorization token generation, and audit event inscription in the WD117 Compliance Framework distributed ledger.

[0035] In a preferred embodiment, the WD116 module 160 implements a tiered consent authorization protocol comprising Tier 1 (patient direct consent), Tier 2 (Proxy Constitutional Appointment surrogate consent), and Tier 3 (emergency clinical necessity authorization). Tier 3 emergency authorization is constitutionally permitted only when immediate intervention is required to prevent serious patient harm and a Proxy Constitutional Appointment holder is unavailable within a constitutionally specified response window not to exceed **300** seconds.

IV. WD071 Eldercare Drift Correction Module

[0036] Referring now to FIG. 7, the WD071 Eldercare Drift Correction module 170 governs the continuous constitutional monitoring of all WM-Series device AI operational behavior within the 8-bed ward enterprise IT environment for the occurrence of Constitutional Drift. Constitutional Drift is defined as any unauthorized expansion of AI inference engine authority, operational scope, or actuator control command issuance beyond the constitutionally permissible operational envelope established by the WD-Series constitutional articles governing each WM-Series device.

[0037] Constitutional Article WD071.1 provides that the WD071 Drift Detection Engine 172 shall continuously evaluate all WM-Series AI inference outputs against the constitutional operational envelope parameters established at device initialization, generating a constitutional drift score for each inference cycle. Constitutional Article WD071.2 provides that any constitutional drift score exceeding the constitutional drift threshold — expressed as a normalized deviation coefficient greater than the constitutionally specified limit — shall immediately trigger a hardware interrupt signal 174 to the affected WM-Series device, suspending AI inference output transmission pending constitutional restoration.

[0038] Constitutional Article WD071.3 provides that concurrent with hardware interrupt generation, the WD071 module 170 shall initiate a Tier 2 escalation procedure 176, notifying the designated clinical supervisor of the Constitutional Drift event within a constitutionally specified notification window not to exceed **120** seconds, and generating a drift flag record for inscription in the WD117 Compliance Framework distributed ledger. Constitutional Article WD071.4 provides that Constitutional Drift restoration shall require dual-authorization from at least two independent clinical

supervisors before the affected WM-Series device AI inference engine is restored to operational status.

[0039] In a preferred embodiment, the WD071 module 170 implements a constitutional drift monitoring cadence for each WM-Series device operating within the 8-bed ward, comprising continuous inference output behavioral analysis, constitutional envelope boundary verification, drift score computation, threshold comparison evaluation, and automated hardware interrupt or escalation initiation. The drift monitoring cadence operates as a hypervisor-level process with constitutional supremacy over all WM-Series device application-layer processes.

V. WD117 Compliance Framework Module

[0040] Referring now to FIG. 6, the WD117 Compliance Framework module 180 governs the comprehensive cryptographic recording of all constitutional enforcement events, Sacred Pause delays, Constitutional Drift flags, biometric unlock events, compliance attestations, and derogation justifications generated by the WD115, WD116, and WD071 modules and the WM-Series hardware devices operating within the 8-bed ward environment.

[0041] The WD117 module 180 comprises a Distributed Ledger Architecture 182 implementing cryptographic immutability, ensuring that all inscribed constitutional governance records cannot be modified, deleted, or fabricated after initial inscription. In a preferred embodiment, the Distributed Ledger Architecture 182 employs a permissioned blockchain architecture accessible to the device manufacturer, designated clinical supervisors, the Health Sciences Authority, and the U.S. Food and Drug Administration upon regulatory request, implementing role-based access control mechanisms.

[0042] Constitutional Article WD117.1 provides that all Sacred Pause delay events — defined as constitutionally mandated execution pauses enforced by the Constitutional Enforcement Engine pending clinician verification via WM-005 iris biometric authentication — shall be recorded in the Distributed Ledger Architecture 182 with timestamped initiation records, pause duration records, and clinician authorization records. Constitutional Article WD117.2 provides that all WD071 Constitutional Drift flags shall be recorded in the Distributed Ledger Architecture 182 with timestamped drift detection records, drift score values, hardware interrupt records, and Tier 2 escalation notification records.

[0043] Constitutional Article WD117.3 provides that the WD117 Regulatory Submission Data Packager 184 shall automatically compile all constitutional compliance attestation records, drift flag records, Sacred Pause records, biometric unlock records, derogation justification records, and constitutional enforcement event logs into a structured regulatory submission data package formatted for submission to the HSA as supporting evidence for a Class B SaMD Pre-Market Submission and to the FDA as supporting evidence for Software as a Medical Device V&V protocol compliance.

[0044] In a preferred embodiment, the WD117 module 180 implements a constitutional post-market surveillance sub-module configured to continuously collect real-world performance data from all WM-Series devices deployed within the 8-bed ward, evaluate collected data against constitutional performance thresholds, and generate constitutional post-market surveillance reports satisfying HSA post-market

requirements for Class B SaMD products and FDA post-market surveillance obligations.

VI. Integrated Ward-Level Constitutional Compliance Workflow

[0045] Referring now to FIG. 2, the integrated ward-level constitutional compliance verification workflow 200 governs all clinical event processing within the 8-bed ward from initial WM-003 detection through regulatory audit logging. The workflow 200 comprises the following constitutional stages executed in hierarchical sequence.

[0046] Stage 1: WM-003 Detection Event. The WM-003 fall prevention LiDAR and thermal sensing system 120 generates a constitutional trigger event upon detection of a fall event, high-risk posture, bed-exit event, or spatial anomaly within the 8-bed ward environment, initiating the constitutional compliance verification workflow 200.

[0047] Stage 2: WD115 Ambient Care Intelligence Privacy Validation. The WD115 Ambient Classification Engine 152 evaluates the WM-003 trigger event data against constitutional Ambient Care Intelligence classification criteria, confirming that the event data constitutes a non-identifiable, clinically purposeful Ambient Care Intelligence representation before permitting downstream processing. Events failing WD115 validation are withheld from downstream clinical systems and are logged as constitutional derogation events in the WD117 Distributed Ledger Architecture 182.

[0048] Stage 3: WD071 Constitutional Drift Verification. The WD071 Drift Detection Engine 172 evaluates the WM-003 AI inference output associated with the trigger event against the constitutional operational envelope parameters, confirming the absence of Constitutional Drift before permitting clinical alert generation. Drift events trigger hardware interrupts and Tier 2 escalation as specified in Constitutional Article WD071.2 and WD071.3.

[0049] Stage 4: Sacred Pause Clinician Verification. Upon constitutional validation of the WM-003 trigger event by WD115 and WD071, the Constitutional Enforcement Engine initiates a Sacred Pause — a constitutionally mandated execution pause — requiring clinician verification via WM-005 iris biometric authentication before any clinical intervention recommendation is transmitted to the clinical output subsystem. The Sacred Pause duration is timestamped and recorded in the WD117 Distributed Ledger Architecture 182.

[0050] Stage 5: WD117 Immutable Ledger Recording. Upon successful clinician verification, or upon constitutionally authorized emergency bypass, all constitutional enforcement events, compliance attestations, Sacred Pause records, and clinical alert outputs associated with the trigger event are inscribed in the WD117 Distributed Ledger Architecture 182 as immutable regulatory audit records.

VII. HSA Class B SaMD and FDA V&V Regulatory Alignment

[0051] Referring now to FIG. 9, the WD-WM Ward Integration System is systematically aligned with HSA Class B SaMD regulatory requirements and FDA Software as a Medical Device V&V protocol requirements through the WD117 Regulatory Alignment Matrix 190. The matrix maps each WD-Series constitutional article to corresponding HSA regulatory requirements, FDA guidance provisions, ISO 14971 risk control

elements, ISO 13485 quality management elements, and IEC 62304 software lifecycle requirements.

[0052] WD115 Ambient Care Intelligence provisions are aligned with HSA SaMD data governance requirements, FDA Software as a Medical Device Guidance data privacy provisions, ISO 14971 Clause 6 risk control implementation requirements, and ISO 13485 Clause 7.1 planning of product realization requirements.

[0053] WD116 Silent Elder Protocols provisions are aligned with HSA SaMD patient dignity and consent requirements, FDA guidance provisions on vulnerable patient population protections, ISO 14971 Clause 4 risk analysis requirements for cognitively impaired patient populations, and ISO 13485 Clause 7.3 design and development requirements.

[0054] WD071 Eldercare Drift Correction provisions are aligned with HSA SaMD AI behavioral governance requirements, FDA Software as a Medical Device predetermined change control plan requirements, ISO 14971 Clause 5 risk evaluation requirements, and IEC 62304 Clause 6 software maintenance requirements.

[0055] WD117 Compliance Framework provisions support the generation of all technical documentation required for an HSA Class B SaMD Pre-Market Submission and FDA V&V protocol compliance evidence package, including software description documentation, clinical evaluation reports, risk management files, post-market surveillance plans, and immutable audit trail records, all derived from or supported by constitutional governance records maintained in the WD117 Distributed Ledger Architecture 182.

Claims

[0056] What is claimed is:

Claim 1. A constitutionally governed enterprise IT integration system for Software as a Medical Device (SaMD) regulatory compliance in an eldercare ward environment comprising:

a WM-001 vital sign monitor operatively coupled to a constitutional vital data acquisition controller;

a WM-003 fall prevention LiDAR and thermal sensing system configured to generate point-cloud vector and thermal matrix data streams;

a WM-005 diagnostic iris and eye scanner comprising an iris biometric authentication engine;

a WD115 Ambient Care Intelligence module configured to classify WM-001 and WM-003 operational outputs as passive, non-identifiable, clinically purposeful Ambient Care Intelligence data;

a WD116 Silent Elder Protocols module configured to enforce a Zero-Default Harm Principle and Proxy Constitutional Appointment governance for cognitively impaired patients;

a WD071 Eldercare Drift Correction module configured to detect Constitutional Drift in WM-Series device AI inference behavior and trigger hardware interrupts or Tier 2 escalations; and

a WD117 Compliance Framework module configured to immutably record all constitutional enforcement events, Sacred Pause delays, drift flags, and biometric unlock events in a cryptographic distributed ledger.

Claim 2. The system of Claim 1, wherein the WM-003 fall prevention LiDAR and thermal sensing system comprises a multi-beam laser emitter, a time-of-flight engine, a point-cloud generation module, a thermal matrix processor, and a sovereignty gate governing sensor output release subject to WD115 constitutional classification.

Claim 3. The system of Claim 1, wherein the WD115 Ambient Care Intelligence module enforces constitutional thermal anonymization protocols and constitutional data minimization constraints limiting sensor data retention to the minimum clinically necessary for the declared clinical purpose.

Claim 4. The system of Claim 1, wherein the WD116 Silent Elder Protocols module activates Zero-Default Harm Principle enforcement upon determination by a cognitive status assessment module that a patient lacks decisional capacity, suspending all non-essential clinical recommendation outputs pending Proxy Constitutional Appointment authorization.

Claim 5. The system of Claim 1, wherein the WM-005 iris biometric authentication engine gates all authorized clinician access to WM-005 diagnostic output data for cognitively impaired patients, generating a constitutional biometric authorization token upon successful iris authentication and recording a biometric unlock event in the WD117 distributed ledger.

Claim 6. The system of Claim 1, wherein the WD071 Eldercare Drift Correction module continuously evaluates WM-Series AI inference outputs against constitutional operational envelope parameters, generating a constitutional drift score for each inference cycle and triggering a hardware interrupt upon detection of a drift score exceeding a constitutionally specified threshold.

Claim 7. The system of Claim 6, wherein the WD071 module initiates a Tier 2 escalation procedure concurrently with hardware interrupt generation, notifying a designated clinical supervisor within a constitutionally specified notification window not to exceed **120** seconds.

Claim 8. The system of Claim 1, wherein the WD117 Compliance Framework module employs a permissioned blockchain architecture implementing cryptographic immutability, accessible to the device manufacturer, designated clinical supervisors, the Health Sciences Authority, and the U.S. Food and Drug Administration upon regulatory request.

Claim 9. The system of Claim 1, wherein the integrated ward-level constitutional compliance verification workflow comprises: WM-003 detection event generation; WD115 Ambient Care Intelligence privacy validation; WD071 Constitutional Drift verification; Sacred Pause clinician verification via WM-005 iris biometric authentication; and WD117 immutable ledger recording.

Claim 10. The system of Claim 9, wherein the Sacred Pause is a constitutionally mandated execution pause enforced by the Constitutional Enforcement Engine pending clinician verification via WM-005 iris biometric authentication, during which all clinical intervention recommendation transmissions are suspended.

Claim 11. The system of Claim 1, wherein the WD116 Silent Elder Protocols module implements a tiered consent authorization protocol comprising Tier 1 patient direct consent, Tier 2 Proxy Constitutional Appointment surrogate consent, and Tier 3 emergency clinical necessity authorization, wherein Tier 3 authorization is permitted only when a Proxy Constitutional Appointment holder is unavailable within a response window not to exceed **300** seconds.

Claim 12. The system of Claim 1, wherein restoration of a WM-Series device AI inference engine following a Constitutional Drift hardware interrupt requires dual-authorization from at least two independent clinical supervisors before operational reinstatement.

Claim 13. The system of Claim 1, wherein the WD117 Regulatory Submission Data Packager automatically compiles constitutional compliance attestation records, drift flag records, Sacred Pause records, biometric unlock records, and derogation justification records into a structured regulatory submission data package formatted for HSA Class B SaMD Pre-Market Submission and FDA Software as a Medical Device Verification and Validation protocol compliance evidence.

Claim 14. The system of Claim 1, wherein the system is deployed across an 8-bed eldercare ward topology wherein each of the eight patient care stations is equipped with a constitutionally governed instance of the WM-001, WM-003, and WM-005 devices, collectively forming a ward-level sensor fusion environment governed by the WD-Series constitutional protocol stack.

Claim 15. A method for constitutionally governed enterprise IT integration of WM-Series medical hardware in an eldercare ward environment comprising:

deploying WM-001 vital sign monitors, WM-003 fall prevention LiDAR and thermal sensing systems, and WM-005 diagnostic iris and eye scanners across an 8-bed ward enterprise IT topology;

classifying all WM-001 and WM-003 operational outputs as Ambient Care Intelligence using a WD115 constitutional classification engine;

enforcing Zero-Default Harm Principle and Proxy Constitutional Appointment governance for cognitively impaired patients using a WD116 Silent Elder Protocols module;

monitoring WM-Series AI inference outputs for Constitutional Drift using a WD071 Eldercare Drift Correction module and triggering hardware interrupts or Tier 2 escalations upon drift detection;

executing a Sacred Pause pending clinician verification via WM-005 iris biometric authentication upon detection of a constitutionally significant clinical event; and

recording all constitutional enforcement events, Sacred Pause delays, drift flags, and biometric unlock events in a WD117 cryptographic distributed ledger.

Claim 16. The method of Claim 15, further comprising compiling a structured regulatory submission data package from WD117 distributed ledger records for submission to the Health Sciences Authority as supporting evidence for a Class B SaMD Pre-Market Submission and to the FDA as Software as a Medical Device Verification and Validation protocol compliance evidence.

Claim 17. The method of Claim 15, wherein classifying all WM-001 and WM-003 operational outputs as Ambient Care Intelligence comprises applying constitutional thermal anonymization protocols and constitutional data minimization constraints to all LiDAR point-cloud vector and thermal matrix data streams prior to downstream clinical inference processing.

Claim 18. A non-transitory computer-readable medium storing instructions that, when executed by one or more processors of an enterprise IT integration system for an 8-bed eldercare ward, cause the system to implement a WD-Series constitutional governance framework comprising:

enforcing WD115 Ambient Care Intelligence classification on all WM-001 and WM-003 sensor outputs;

activating WD116 Zero-Default Harm Principle and Proxy Constitutional Appointment governance for cognitively impaired ward patients;

continuously monitoring WM-Series AI inference behavior for Constitutional Drift using WD071 and triggering hardware interrupts upon drift threshold exceedance;

executing Sacred Pause enforcement requiring WM-005 iris biometric clinician authentication before clinical intervention recommendation transmission; and

recording all constitutional governance events in a WD117 cryptographically immutable distributed ledger generating HSA and FDA regulatory submission data packages.

Claim 19. The non-transitory computer-readable medium of Claim 18, wherein monitoring WM-Series AI inference behavior for Constitutional Drift comprises computing a constitutional drift score for each AI inference cycle and comparing the score against a constitutionally specified drift threshold, wherein exceedance triggers simultaneous hardware interrupt generation and Tier 2 clinical supervisor notification.

Claim 20. A constitutional governance device for enterprise eldercare ward integration under Health Sciences Authority Class B SaMD classification and FDA Software as a Medical Device Verification and Validation protocol compliance, the device comprising:

one or more WM-001 physiological sensor arrays configured to acquire eldercare patient vital sign data;

one or more WM-003 LiDAR and thermal sensing arrays configured to generate constitutionally classified Ambient Care Intelligence representations of the ward spatial environment;

a WM-005 iris biometric authentication engine configured to gate authorized clinician access to sensitive diagnostic outputs;

a WD-Series constitutional governance protocol stack comprising WD115, WD116, WD071, and WD117 modules operatively governing all WM-Series device operations; and

a WD117 cryptographic distributed ledger recording all constitutional enforcement events in an immutable regulatory audit trail.

Abstract

An integrated WD-Series constitutionally governed enterprise IT architecture for WM-Series medical hardware deployment in an 8-bed eldercare ward is disclosed, comprising the WM-001 vital sign monitor, WM-003 fall prevention LiDAR and thermal sensing system, and WM-005 diagnostic iris and eye scanner, governed by the WD115 Ambient Care Intelligence module, WD116 Silent Elder Protocols module, WD071 Eldercare Drift Correction module, and WD117 Compliance Framework module. The WD115 module classifies all LiDAR point-cloud vector and thermal matrix sensing outputs as passive, non-identifiable, clinically purposeful Ambient Care Intelligence to preserve patient dignity. The WD116 module enforces a Zero-Default Harm Principle and Proxy Constitutional Appointment governance for cognitively impaired patients, gating clinician access through WM-005 iris biometric authentication. The WD071 module continuously monitors for Constitutional Drift in WM-Series AI inference behavior, triggering hardware interrupts and Tier 2 escalations upon drift detection. An integrated ward-level constitutional compliance workflow governs WM-003 detection, WD115 privacy validation, WD071 drift verification, Sacred Pause clinician verification via WM-005, and WD117 immutable ledger recording. The WD117 module records all constitutional enforcement events, Sacred Pause delays, drift flags, and biometric unlock events in a cryptographically immutable distributed ledger, generating structured regulatory submission data packages satisfying ISO 14971 risk management standards, ISO 13485 quality management standards, IEC 62304 software lifecycle requirements, HSA Class B SaMD Pre-Market Submission requirements, and FDA Software as a Medical Device Verification and Validation protocol compliance requirements.

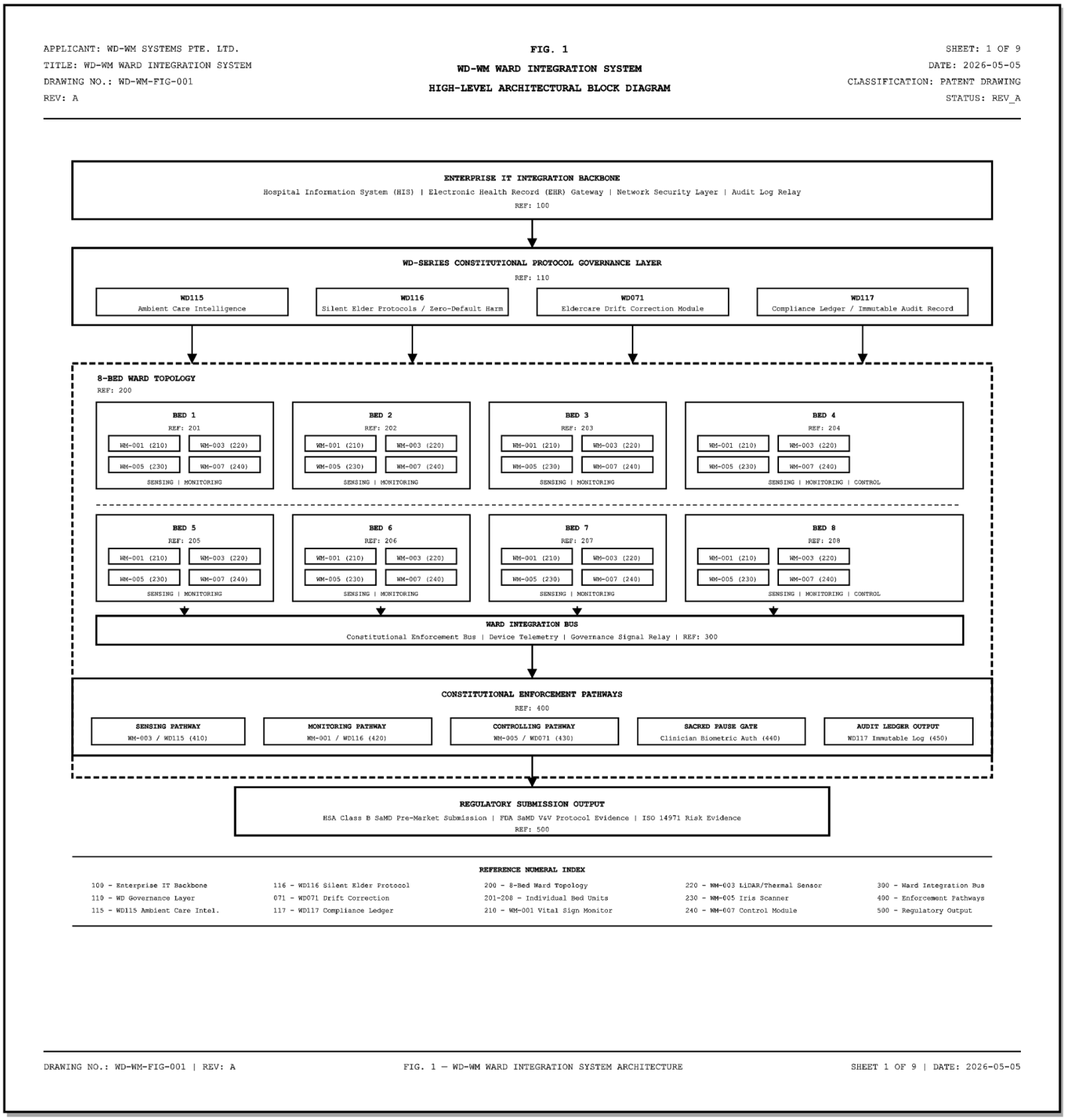


FIG. 1 is a high-level architectural block diagram of the WD-WM Ward Integration System illustrating the 8-bed ward topology, WM-Series device deployment positions, WD-Series protocol governance layers, enterprise IT integration backbone, and constitutional enforcement pathways across sensing, monitoring, and controlling subsystems.

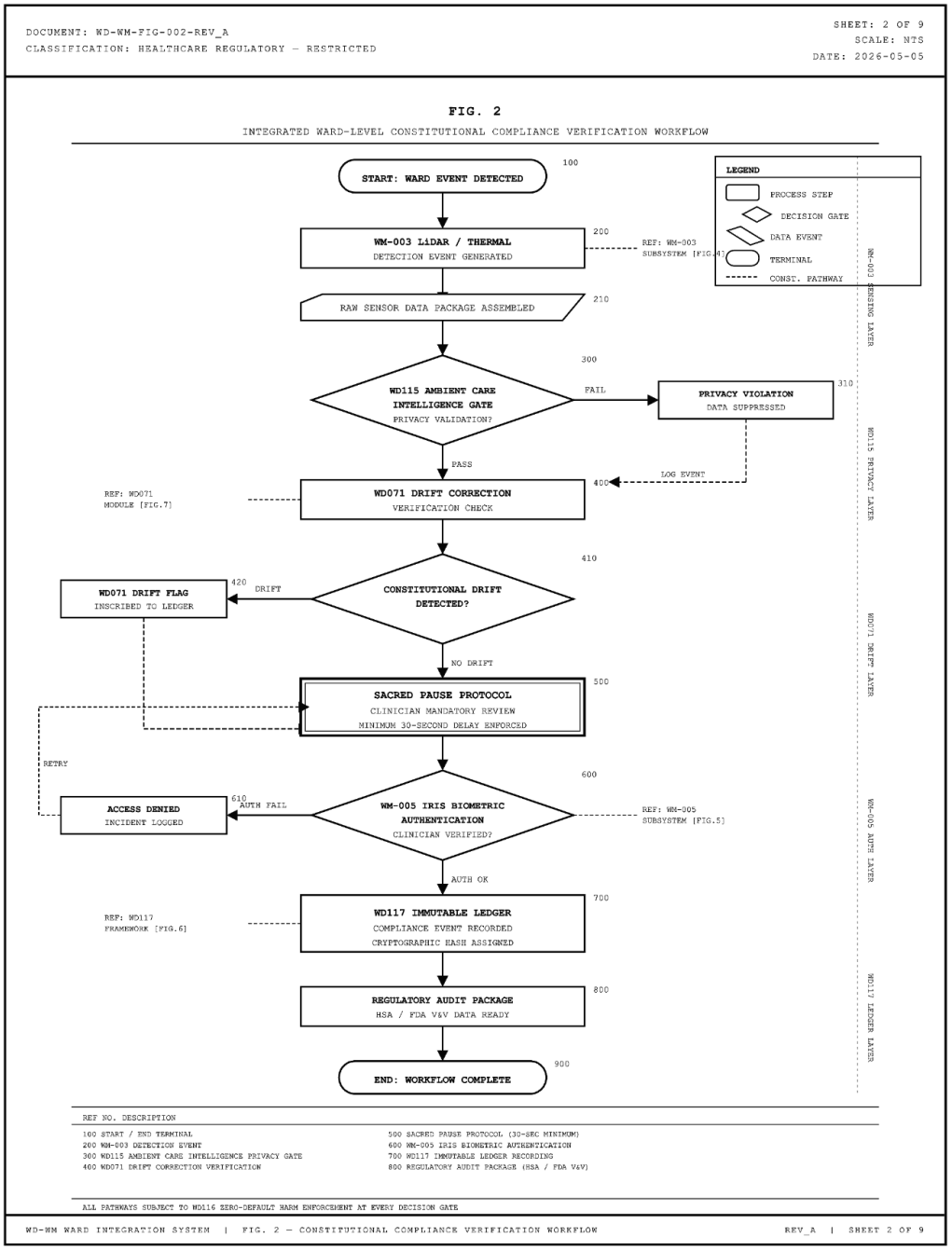


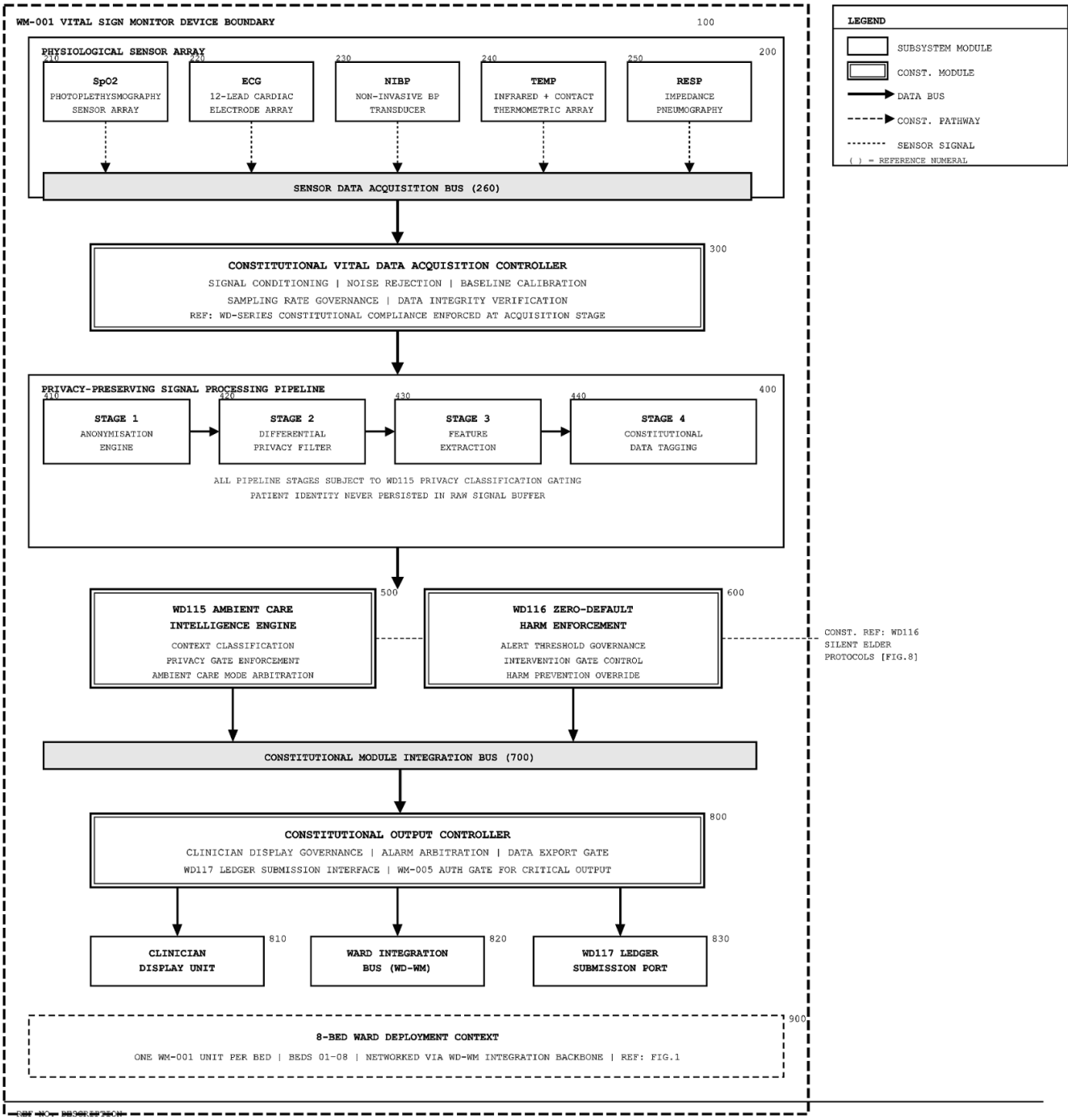
FIG. 2 — FORMAL CAPTION

FIG. 2 is a flowchart illustrating the integrated ward-level constitutional compliance verification workflow (100–900), beginning with WM-003 LiDAR and thermal detection event generation (200), proceeding through WD115 Ambient Care Intelligence privacy validation gate (300), WD071 Drift Correction verification and drift flag inscription (400, 420), Sacred Pause clinician mandatory review with minimum 30-second enforcement delay (500), WM-005 iris biometric clinician authentication (600), and culminating in WD117 immutable ledger compliance event recording (700) with cryptographic hash assignment and regulatory audit package generation (800) for HSA Pre-Market Submission and FDA V&V protocol evidence.

FIG. 2 is a flowchart illustrating the integrated ward-level constitutional compliance verification workflow, beginning with WM-003 detection events, proceeding through WD115 Ambient Care Intelligence privacy validation, WD071 Drift Correction verification, Sacred Pause clinician verification via WM-005 iris biometric authentication, and culminating in WD117 immutable ledger recording for regulatory audit.

FIG. 3

WM-001 VITAL SIGN MONITOR — CONSTITUTIONAL SUBSYSTEM SCHEMATIC



100 WM-001 DEVICE BOUNDARY
200 PHYSIOLOGICAL SENSOR ARRAY
210 SpO2 PHOTOPLETHYSMOGRAPHY SENSOR
220 ECG 12-LEAD CARDIAC ELECTRODE ARRAY
230 NIBP NON-INVASIVE BP TRANSDUCER
240 INFRARED + CONTACT THERMOMETRIC ARRAY
250 IMPEDANCE PNEUMOGRAPHY RESP SENSOR
260 SENSOR DATA ACQUISITION BUS
300 CONSTITUTIONAL VITAL DATA ACQUISITION CONTROLLER
400 PRIVACY-PRESERVING SIGNAL PROCESSING PIPELINE
500 WD115 AMBIENT CARE INTELLIGENCE ENGINE
600 WD116 ZERO-DEFAULT HARM ENFORCEMENT MODULE
700 CONSTITUTIONAL MODULE INTEGRATION BUS
800 CONSTITUTIONAL OUTPUT CONTROLLER
810 CLINICIAN DISPLAY UNIT
820 WARD INTEGRATION BUS (WD-WM BACKBONE)
830 WD117 LEDGER SUBMISSION PORT
900 8-BED WARD DEPLOYMENT CONTEXT

ALL MODULES SUBJECT TO WD116 ZERO-DEFAULT HARM PRINCIPLE | ALL OUTPUTS GATED BY CONSTITUTIONAL ENFORCEMENT LAYER | REF: WD-SERIES GOVERNANCE

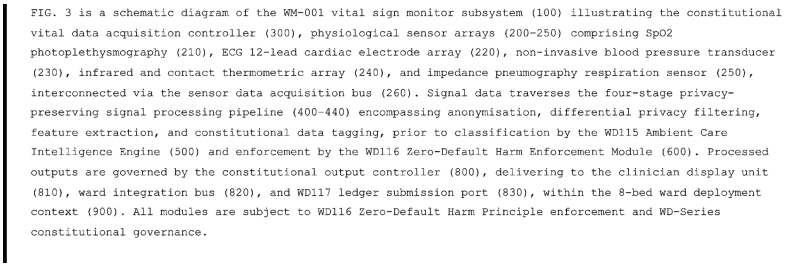
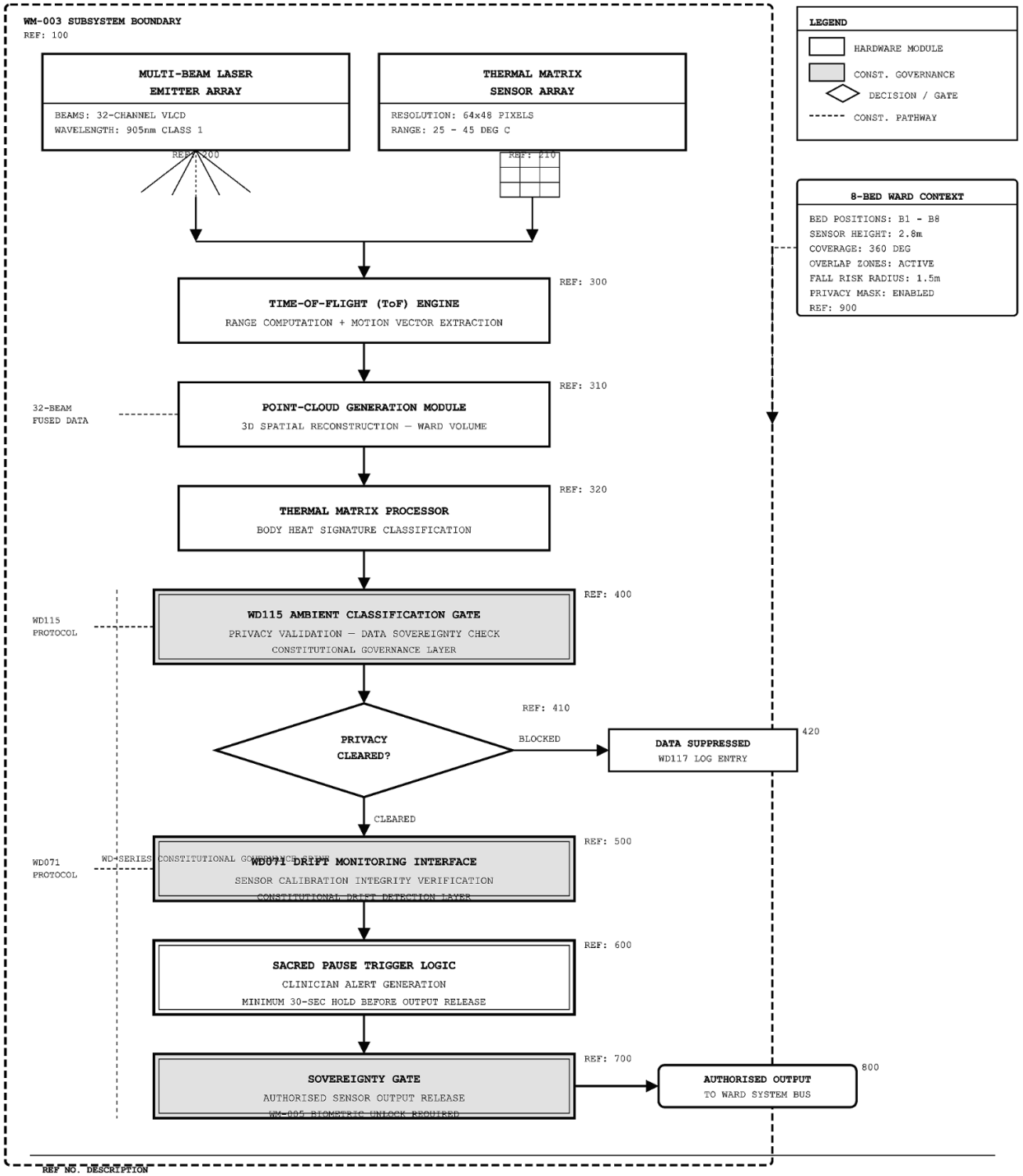


FIG. 3 is a schematic diagram of the WM-001 vital sign monitor subsystem (100) illustrating the constitutional vital data acquisition controller (300), physiological sensor arrays (200–250) comprising SpO2 photoplethysmography (210), ECG 12-lead cardiac electrode array (220), non-invasive blood pressure transducer (230), infrared and contact thermometric array (240), and impedance pneumography respiration sensor (250), interconnected via the sensor data acquisition bus (260). Signal data traverses the four-stage privacy-preserving signal processing pipeline (400–440) encompassing anonymisation, differential privacy filtering, feature extraction, and constitutional data tagging, prior to classification by the WD115 Ambient Care Intelligence Engine (500) and enforcement by the WD116 Zero-Default Harm Enforcement Module (600). Processed outputs are governed by the constitutional output controller (800), delivering to the clinician display unit (810), ward integration bus (820), and WD117 ledger submission port (830), within the 8-bed ward deployment context (900). All modules are subject to WD116 Zero-Default Harm Principle enforcement and WD-Series constitutional governance.

FIG. 3 is a schematic diagram of the WM-001 vital sign monitor subsystem illustrating the constitutional vital data acquisition controller, physiological sensor arrays, privacy-preserving signal processing pipeline, WD115 ambient classification engine, and WD116 Zero-Default Harm enforcement module as integrated within the 8-bed ward environment.

FIG. 4

WM-003 FALL PREVENTION LiDAR AND THERMAL SENSING SUBSYSTEM



REF NO.	DESCRIPTION
100	WM-003 SUBSYSTEM BOUNDARY
200	MULTI-BEAM LASER EMITTER ARRAY (32-CH, 905nm)
210	THERMAL MATRIX SENSOR ARRAY (64x48)
300	TIME-OF-FLIGHT ENGINE
310	POINT-CLOUD GENERATION MODULE
320	THERMAL MATRIX PROCESSOR
400	WD115 AMBIENT CLASSIFICATION GATE
500	WD071 DRIFT MONITORING INTERFACE
600	SACRED PAUSE TRIGGER LOGIC
700	SOVEREIGNTY GATE / 800 AUTHORISED OUTPUT

ALL GOVERNANCE LAYERS SUBJECT TO WD116 ZERO-DEFAULT HARM ENFORCEMENT. DASHED FILL DENOTES CONSTITUTIONAL MODULE.
OUTPUT RELEASE REQUIRES WM-005 BIOMETRIC UNLOCK AT SOVEREIGNTY GATE (REF: 700). CROSS-REF: FIG. 5.

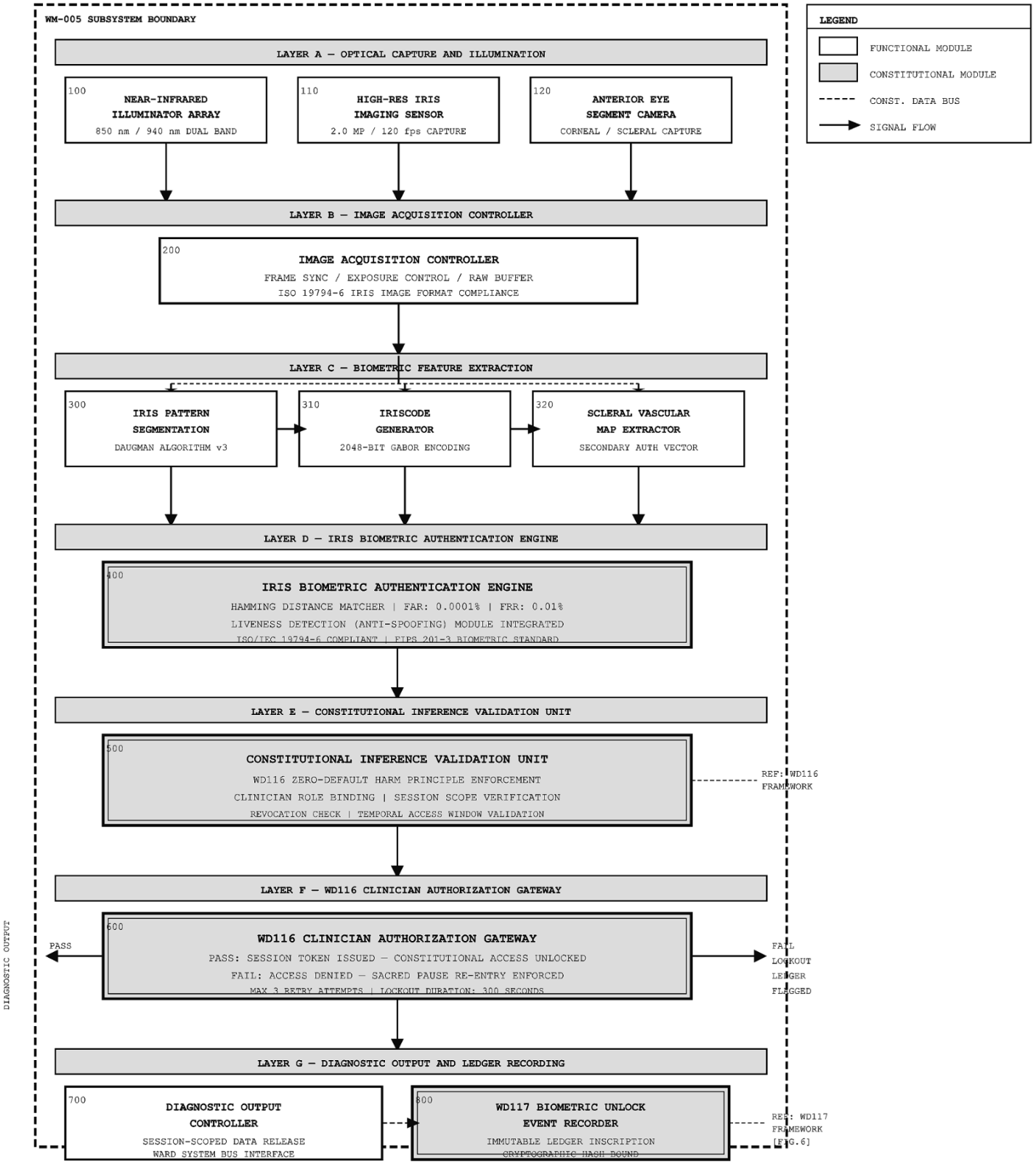
FIG. 4 — FORMAL CAPTION

FIG. 4 is a block diagram of the WM-003 fall prevention LiDAR and thermal sensing subsystem (100) illustrating the 32-channel multi-beam laser emitter array (200) operating at 905nm Class 1 wavelength, the 64x48 thermal matrix sensor array (210), time-of-flight engine (300) for range computation and motion vector extraction, point-cloud generation module (310) for three-dimensional spatial reconstruction of the ward volume, thermal matrix processor (320) for body heat signature classification, WD115 Ambient Care Intelligence ambient classification gate (400) for privacy validation and data sovereignty enforcement, WD071 drift monitoring interface (500) for sensor calibration integrity verification and constitutional drift detection, Sacred Pause trigger logic (600) enforcing a minimum 30-second clinician alert hold before output release, and sovereignty gate (700) governing final authorised sensor output release (800) to the ward system bus, requiring WM-005 iris biometric unlock. The 8-bed ward deployment context is indicated at reference (900). All governance layers operate under WD116 Zero-Default Harm enforcement. Constitutional modules are indicated by shaded fill and double-border enclosure.

FIG. 4 is a block diagram of the WM-003 fall prevention LiDAR and thermal sensing subsystem illustrating the multi-beam laser emitter array, time-of-flight engine, point-cloud generation module, thermal matrix processor, WD115 ambient classification gate, WD071 drift monitoring interface, Sacred Pause trigger logic, and sovereignty gate governing sensor output release.

FIG. 5

WM-005 DIAGNOSTIC IRIS AND EYE SCANNER SUBSYSTEM



REF NO.	DESCRIPTION
100	NEAR-INFRARED ILLUMINATOR ARRAY (850nm / 940nm)
110	HIGH-RESOLUTION IRIS IMAGING SENSOR (2.0 MP / 120 fps)
120	ANTERIOR EYE SEGMENT CAMERA (CORNEAL / SCLERAL)
200	IMAGE ACQUISITION CONTROLLER (ISO 19794-6)
300	IRIS PATTERN SEGMENTATION (DAUGMAN ALGORITHM v3)
310	IRISCODE GENERATOR (2048-BIT GABOR ENCODING)
320	SCLERAL VASCULAR MAP EXTRACTOR
400	IRIS BIOMETRIC AUTH ENGINE | 500 CONST. INFERENCE VALIDATION UNIT

FIG. 5 — FORMAL CAPTION

FIG. 5 is a schematic block diagram of the WM-005 diagnostic iris and eye scanner subsystem illustrating seven constitutional processing layers. Layer A (100, 110, 120) comprises the near-infrared illuminator array, high-resolution iris imaging sensor, and anterior eye segment camera. Layer B (200) provides the image acquisition controller operating under ISO 19794-6 iris image format compliance. Layer C (300, 310, 320) encompasses biometric feature extraction including iris pattern segmentation via Daugman Algorithm v3, IrisCode generation via 2048-bit Gabor encoding, and scleral vascular map extraction as a secondary authentication vector. Layer D (400) is the iris biometric authentication engine integrating Hamming distance matching and liveness detection anti-spoofing module. Layer E (500) is the constitutional inference validation unit enforcing WD116 Zero-Default Harm Principle, clinician role binding, session scope verification, and temporal access window validation. Layer F (600) is the WD116 clinician authorization gateway governing authenticated session token issuance and Sacred Pause re-entry enforcement on authentication failure. Layer G (700, 800) provides the diagnostic output controller for session-scoped ward system bus data release and the WD117 biometric unlock event recorder for immutable ledger inscription with cryptographic hash binding. Cross-reference: FIG. 4 (WM-003), FIG. 6 (WD117).

FIG. 5 is a schematic diagram of the WM-005 diagnostic iris and eye scanner subsystem illustrating the iris biometric authentication engine, WD116 clinician authorization gateway, diagnostic output controller, constitutional inference validation unit, and WD117 biometric unlock event recorder.

FIG. 6

WM-006 Patient-Centric Constitutional Data Ledger

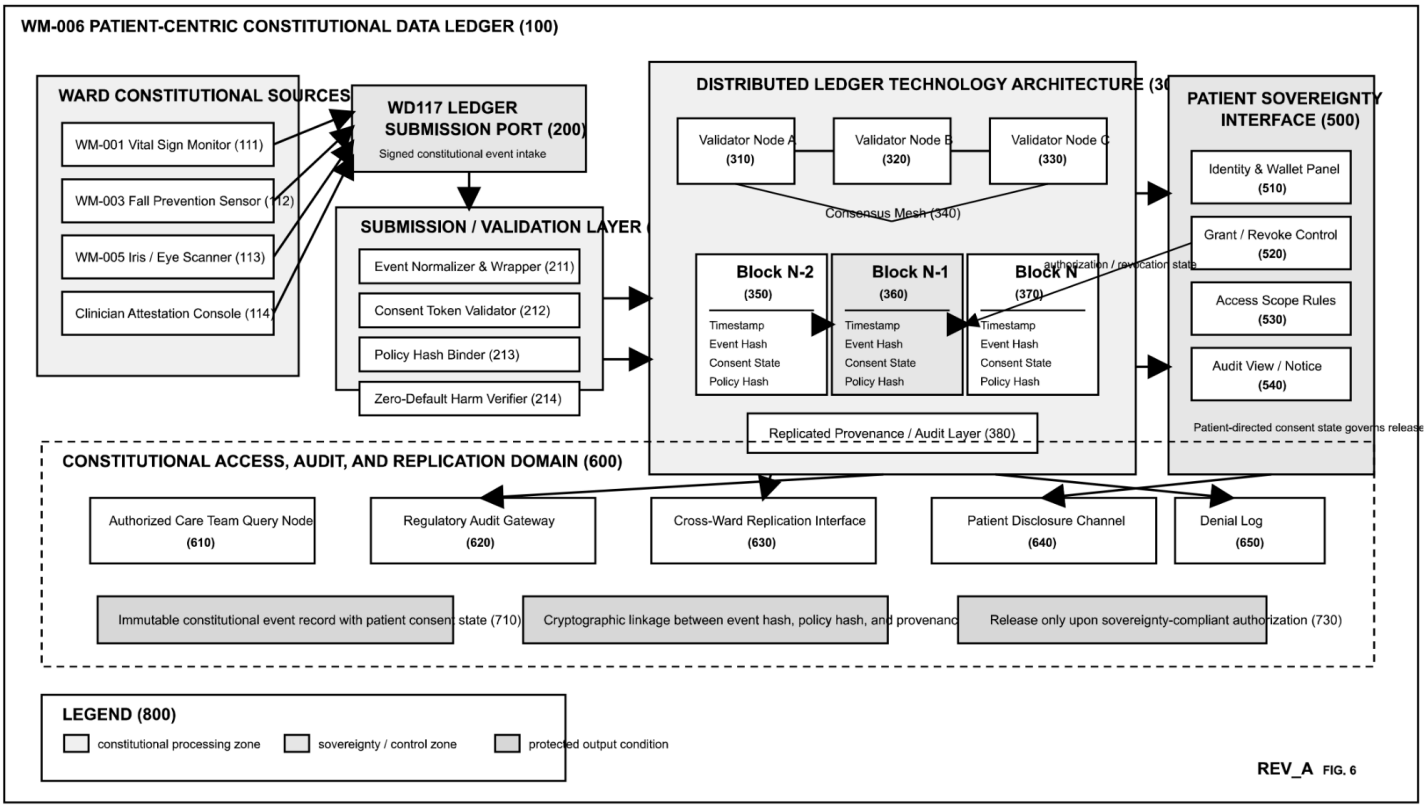


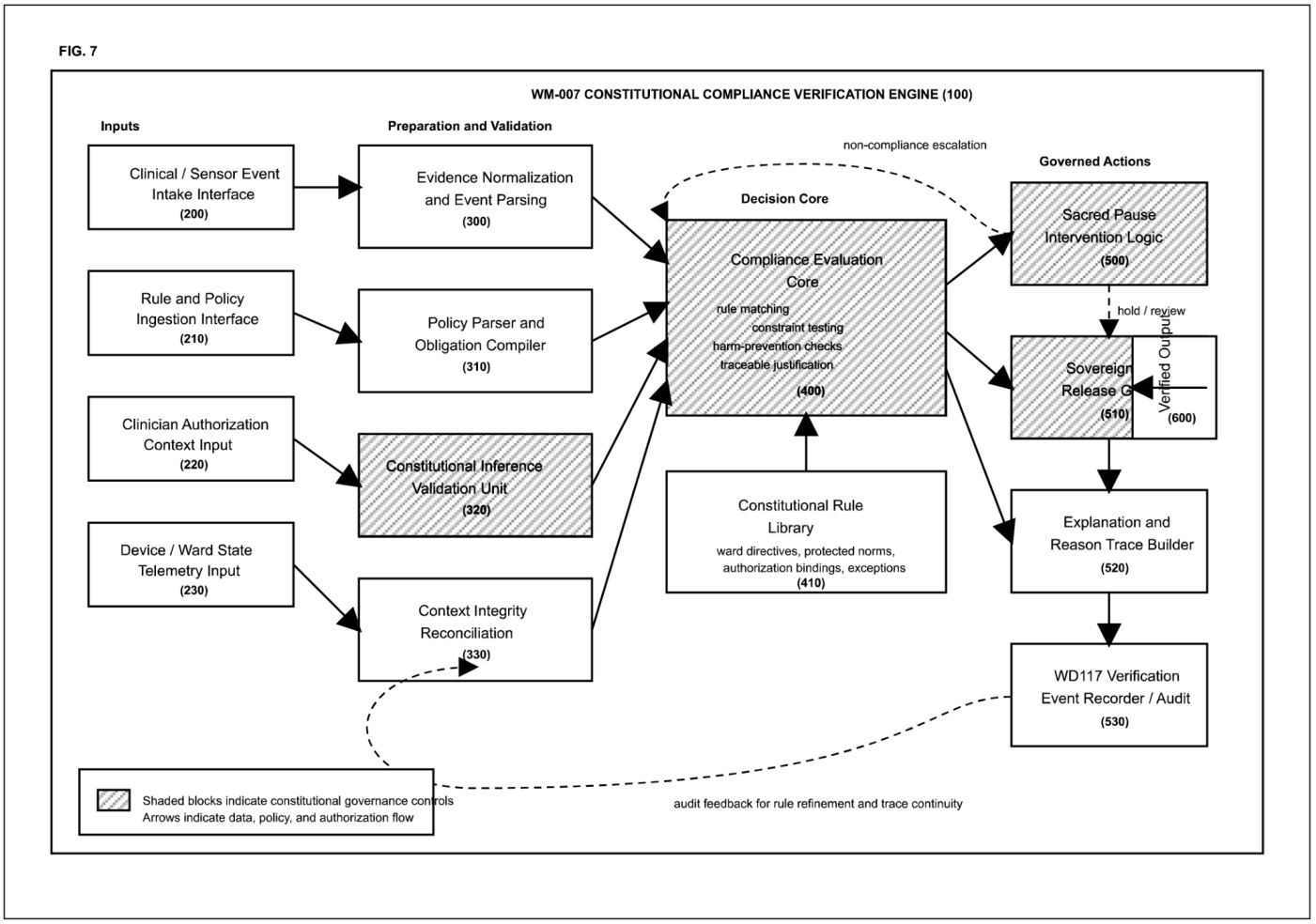
FIG. 6 is a schematic diagram of the **WM-006 Patient-Centric Constitutional Data Ledger** illustrating ward constitutional data sources **(110)**, a **WD117 ledger submission port (200)**, a submission and validation layer **(210)**, a distributed ledg technology architecture **(300)** having validator nodes **(310, 320, 330)**, consensus mesh **(340)**, chained constitutional data blocks **(350, 360, 370)**, a replicated provenance and audit layer **(380)**, and a **patient sovereignty interface (500)** includi identity, grant/revoke, scope-control, and audit-view functions **(510–540)**. The figure further illustrates constitutional access, audit, and replication domain components **(600)** configured to permit disclosure only upon sovereignty-compliant authorizatic while recording immutable constitutional event history and denial conditions.

``` ## Formal Caption **FIG. 6** is a schematic diagram of the **WM-006 Patient-Centric Constitutional Data Ledger** illustrating the distributed ledger technology architecture, constitutional data blocks, **WD117 ledger submission port**, and **patient sovereignty interface**, wherein constitutional healthcare events are normalized, validated, cryptographically bound to policy state, committed to replicated ledger blocks, and selectively disclosed only under patient-authorized constitutional governance. ## Support Notes - **Black-and-white, patent-style layout** maintained. - **Reference numerals** are embedded throughout the drawing. - The file is **standalone HTML** with inline SVG and no external dependencies. - The structure is aligned for the continuing **REV_A** figure set. **FIG. 6 — REV_A** is complete. If you want, I will proceed directly to **FIG. 7**.

**FIG. 6** is a data flow diagram of the WD117 Compliance Framework distributed ledger architecture illustrating cryptographic immutability mechanisms, constitutional enforcement event recording, Sacred Pause delay timestamping, drift flag inscription, biometric unlock logging, compliance attestation storage, and regulatory submission data packaging for HSA Pre-Market Submission and FDA V&V protocol evidence.
```

FIG. 7 — WM-007 Constitutional Compliance Verification Engine

Standalone black-and-white patent-style schematic — REV_A



Formal Caption. FIG. 7 is a schematic block diagram of the **WM-007 constitutional compliance verification engine (100)** illustrating a clinical/sensor event intake interface **(200)**, rule and policy ingestion interface **(210)**, clinician authorization context input **(220)**, device/ward state telemetry input **(230)**, evidence normalization and event parsing module **(300)**, policy parser and obligation compiler **(310)**, constitutional inference validation unit **(320)**, context integrity reconciliation module **(330)**, compliance evaluation core **(400)**, constitutional rule library **(410)**, sacred pause intervention logic **(500)**, sovereignty release gate **(510)**, explanation and reason trace builder **(520)**, WD117 verification event recorder/audit module **(530)**, and verified output interface **(600)**, wherein shaded elements designate constitutional governance layers controlling evaluation, escalation, release, and traceability.

FIG. 7 is a process flow diagram of the WD071 Eldercare Drift Correction module illustrating Constitutional Drift detection logic, hardware interrupt generation pathways, Tier 2 escalation protocols, drift flag recording, and constitutional restoration procedures for WM-Series device governance.

FIG. 8 — WD-WM Ward Integration System Architecture

Secure data flow and constitutional compliance checkpoints between subsystem modules

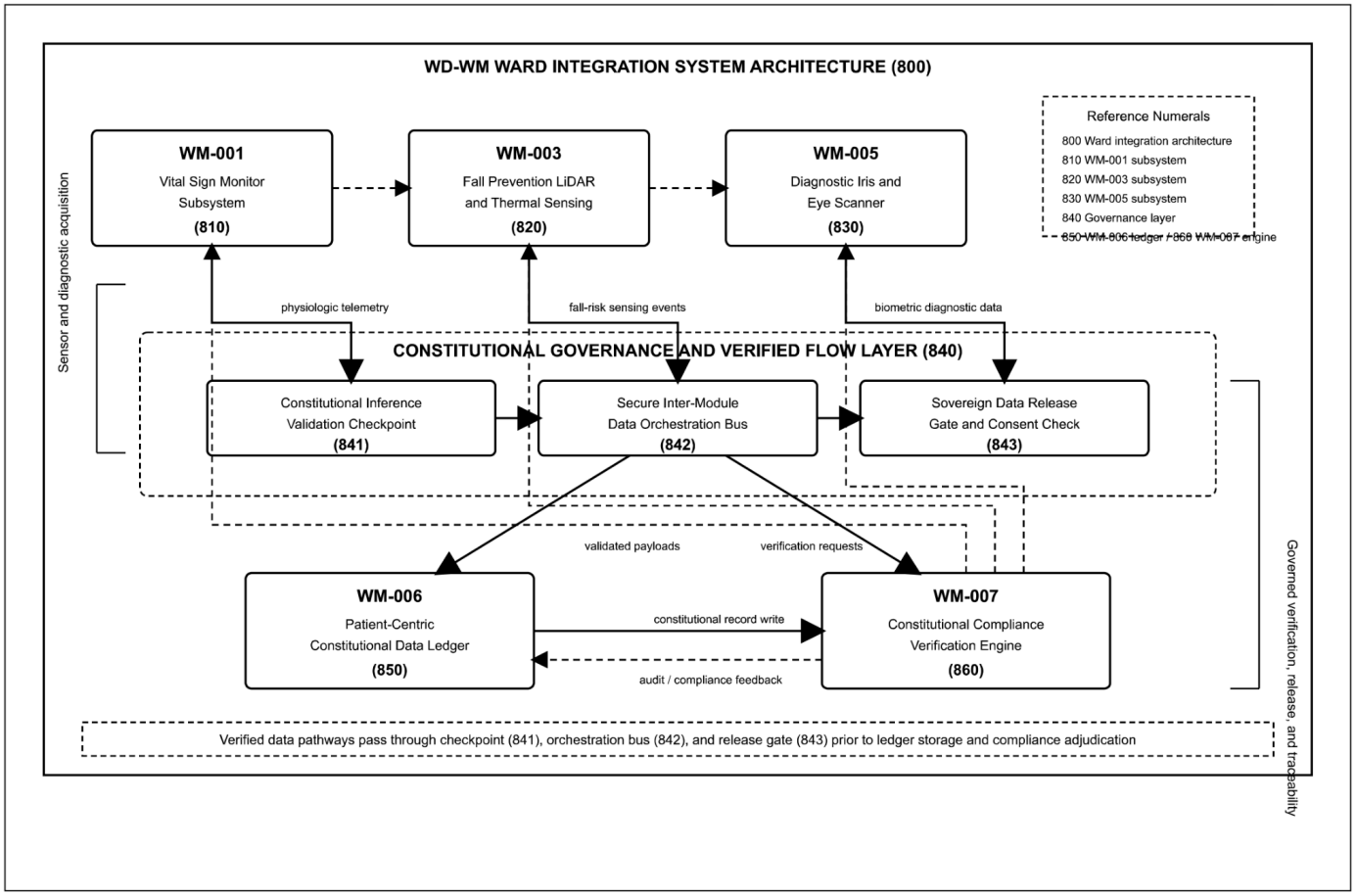


FIG. 8 is a schematic block diagram of the **WD-WM Ward Integration System Architecture (800)** illustrating secure data flow and constitutional compliance checkpoints between the **WM-001 Vital Sign Monitor Subsystem (810)**, the **WM-003 Fall Prevention LiDAR and Thermal Sensing Subsystem (820)**, the **WM-005 Diagnostic Iris and Eye Scanner Subsystem (830)**, the **WM-006 Patient-Centric Constitutional Data Ledger (850)**, and the **WM-007 Constitutional Compliance Verification Engine (860)**. A constitutional governance and verified flow layer **(840)** includes a constitutional inference validation checkpoint **(841)**, a secure inter-module data orchestration bus **(842)**, and a sovereign data release gate and consent check **(843)**, such that subsystem outputs are validated before ledger persistence, compliance adjudication, and controlled release. Solid arrows denote primary verified data exchange pathways, while dashed arrows denote supervisory, audit, and feedback pathways.

FIG. 8 is a schematic diagram of the WD116 Silent Elder Protocols module illustrating the Zero-Default Harm Principle enforcement engine, cognitive status assessment module, Proxy Constitutional Appointment registry, tiered consent authorization protocol, and WM-005 iris biometric authentication integration for clinician access gating.

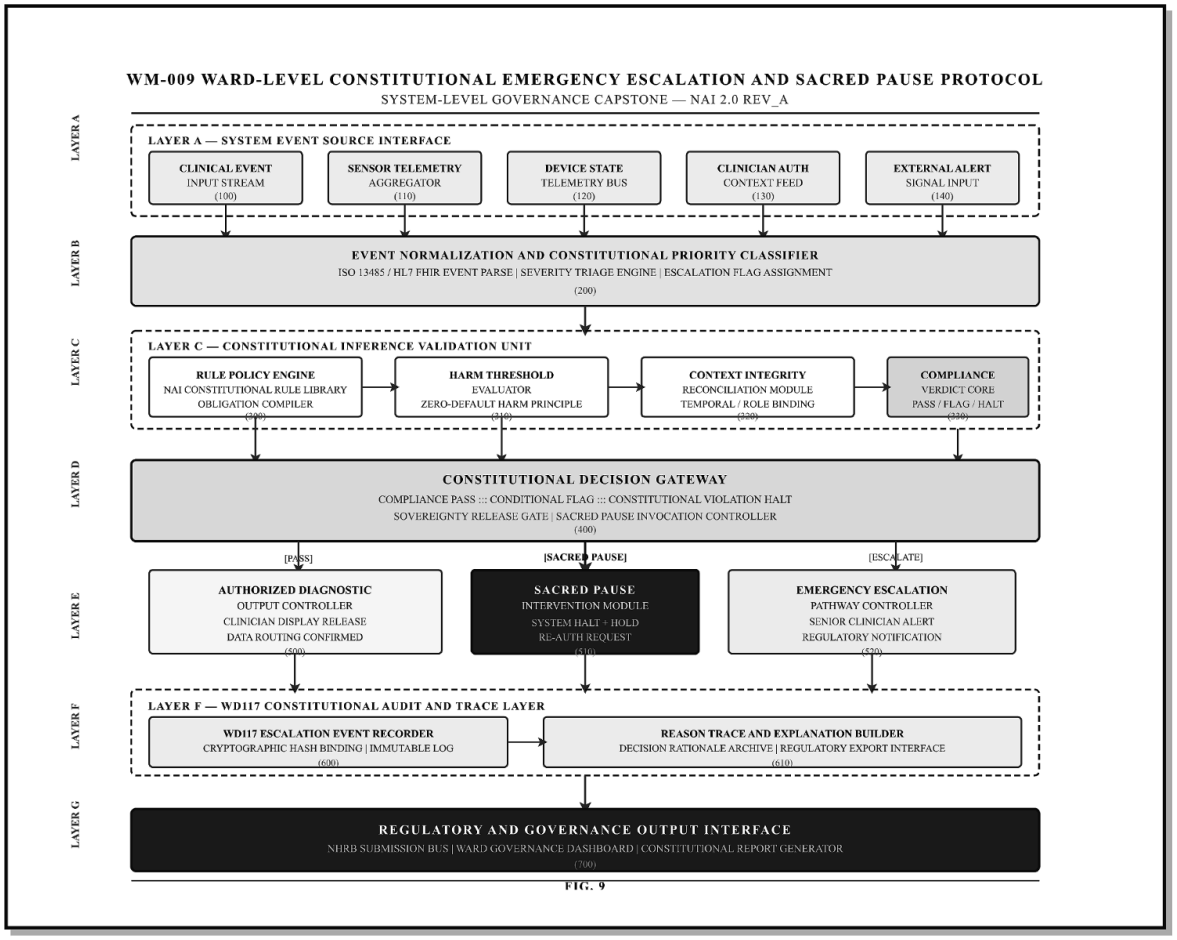


FIG. 9 — FORMAL CAPTION

FIG. 9 is a schematic block diagram of the **WM-009 Ward-Level Constitutional Emergency Escalation and Sacred Pause Protocol (100)** illustrating seven constitutional processing layers: **Layer A** — system event source interface comprising clinical event input stream, sensor telemetry aggregator, device state telemetry bus, clinician authorization context feed, and external alert signal input (100–140); **Layer B** — event normalization and constitutional priority classifier incorporating ISO 13485 / HL7 FHIR event parsing, severity triage engine, and escalation flag assignment (200); **Layer C** — constitutional inference validation unit comprising rule policy engine with NAI constitutional rule library and obligation compiler, harm threshold evaluator enforcing the Zero-Default Harm Principle, context integrity reconciliation module with temporal and role binding, and compliance verdict core issuing Pass, Flag, or Halt verdicts (300–330); **Layer D** — constitutional decision gateway incorporating sovereignty release gate and sacred pause invocation controller, routing events to compliance pass, sacred pause, or escalation pathways (400); **Layer E** — three-path output layer comprising authorized diagnostic output controller with clinician display release and confirmed data routing (500), sacred pause intervention module enforcing system halt, hold, and re-authentication request (510), and emergency escalation pathway controller with senior clinician alert and regulatory notification (520); **Layer F** — WD117 constitutional audit and trace layer comprising the WD117 escalation event recorder with cryptographic hash binding and immutable log generation, and the reason trace and explanation builder with decision rationale archive and regulatory export interface (600–610); and **Layer G** — regulatory and governance output interface providing NHRB submission bus, ward governance dashboard, and constitutional report generator (700); wherein shaded elements designate constitutional enforcement zones, and the Sacred Pause Intervention Module (510) represents the primary constitutional safety enforcement node of the WM-009 subsystem.

FIG. 9 is a diagram of the HSA Class B SaMD and FDA V&V Regulatory Alignment Matrix, mapping each WD-Series constitutional protocol to corresponding HSA regulatory requirements, FDA SaMD guidance provisions, ISO 14971 risk control elements, ISO 13485 quality management elements, and IEC 62304 software lifecycle requirements.

WM-Series 8-Bed Ward Enterprise IT Implementation FDA/HSA Verification & Validation Protocols

Submission Support Package: Workflow Diagram + V&V Protocols

Document status: Draft for engineering, regulatory, and quality review. Not a legal or regulatory opinion. Final predicate selection, product code, and classification should be confirmed by regulatory counsel or a qualified FDA/HSA consultant.

1. Scope and Source Basis

This package converts the WM-Series 8-bed ward mind map and patent content into a linear FDA/HSA workflow and a verification and validation protocol set. The package is intended to support device description, software architecture, risk management, and V&V planning.

Item	Description
Device family	WM-001 vital sign monitor; WM-003 fall prevention LiDAR/thermal sensing; WM-005 iris/eye scanner
Governance protocols	WD115 Ambient Care Intelligence; WD116 Silent Elder Protocols; WD071 Eldercare Drift Correction; WD117 Compliance Framework
Ward scope	8-bed eldercare ward enterprise IT topology with constitutional verification workflow
Regulatory scope	HSA Class B SaMD and FDA Software as a Medical Device verification and validation evidence
Standards referenced	ISO 14971, ISO 13485, IEC 62304, HSA SaMD, FDA V&V documentation

2. Principle of Operation Workflow

The operational workflow is linear with controlled decision gates. Rectangles represent tasks; diamonds represent decision points. Exception branches are routed to fail-safe, escalation, or immutable logging pathways.

Step	Task	Description	Decision Gate	Exception Path
1	System initialization	Load WD-Series governance protocols and verify 8-bed ward readiness	System ready?	No -> fail-safe and supervisor alert
2	Ward data acquisition	Acquire WM-001 vital signs and WM-003 LiDAR/thermal sensing data	Data streams available?	No -> monitoring degraded state
3	WD115 ambient classification	Convert sensing outputs into passive, non-identifiable ambient care intelligence	Privacy validation passed?	No -> withhold output and log derogation
4	Event detection	Identify fall, high-risk posture, bed-exit event, or spatial anomaly	Clinical trigger detected?	No -> passive monitoring loop
5	WD071 drift verification	Assess inference output against constitutional operational envelope	Drift within threshold?	No -> hardware interrupt and Tier 2 escalation
6	WD116 silent elder protocol	Apply zero-default harm, proxy appointment, and consent pathway checks	Authorization pathway valid?	No -> suspend non-essential recommendation
7	Sacred Pause + WM-005 verification	Pause before output and require clinician verification with biometric unlock	Clinician authenticated?	No -> reject and log
8	Controlled clinical output	Transmit alert, recommendation, or environmental support only after validation	System integrity OK?	No -> Sovereign Brake / safe state
9	WD117 ledger and package	Record delay, drift flag, biometric unlock, event trace, and regulatory evidence	Package complete?	No -> remediation workflow

3. Master Traceability Matrix

Req ID	Requirement	Hazard	Risk Control	V&V ID	Standard
REQ-001	Initialize enterprise IT backbone and ward topology	Loss of monitoring across bed stations	Self-check, configuration verification, fail-safe state	VV-001	IEC 62304, ISO 14971
REQ-002	Acquire WM-001 vital signs and WM-003 LiDAR/thermal data	Missing or corrupted sensing data	Sensor availability check, acquisition watchdog	VV-002	IEC 62304
REQ-003	Apply WD115 ambient care classification	Privacy breach or identifiable data exposure	Data minimization, ambient classification, output suppression	VV-003	ISO 14971, HSA/FDA privacy
REQ-004	Detect fall/posture/bed-exit event	Missed fall or false alert	Scenario testing, threshold validation	VV-004	ISO 14971
REQ-005	Perform WD071 drift verification	Uncontrolled AI behavior or authority drift	Drift scoring, threshold interrupt, Tier 2 escalation	VV-005	IEC 62304, ISO 14971
REQ-006	Apply WD116 consent and zero-default harm rules	Unauthorized recommendation for cognitively impaired patient	Consent tier checks, proxy appointment verification	VV-006	IEC 62366, ISO 14971
REQ-007	Enforce Sacred Pause before clinical output	Clinician bypass or automation bias	Timed execution hold, clinician verification gate	VV-007	IEC 62304
REQ-008	Authenticate clinician through WM-005 iris/eye scanner	Unauthorized access to diagnostic output	Biometric unlock, role verification, audit event	VV-008	IEC 62366, cybersecurity
REQ-009	Generate controlled clinical output only after validation	Unsafe output or unintended action	Allow/reject/escalate logic, no autonomous treatment	VV-009	ISO 14971
REQ-010	Record all governance events in	Missing audit evidence	Immutable ledger, event hash,	VV-010	ISO 13485, FDA

	WD117 ledger		timestamp verification		documentation
REQ-011	Generate HSA/FDA V&V package	Incomplete regulatory evidence	Regulatory data packager and review checklist	VV-011	HSA/FDA, ISO 13485
REQ-012	Maintain fail-safe response and lockout	Unsafe restart or failure propagation	Safe state transition, supervisor notification, lockout	VV-012	IEC 60601, ISO 14971
REQ-013	Verify 8-bed multi-station performance	Cross-bed data routing or latency failure	Ward topology integration test	VV-013	IEC 62304
REQ-014	Verify local-only/privacy controls	Cloud/network leakage or unintended transmission	Network isolation, no camera/audio claim checks	VV-014	Cybersecurity, privacy
REQ-015	Validate human factors for clinician workflow	Use error or delayed response	Formative/summative usability validation	VV-015	IEC 62366

4. V&V Protocol Set

VV-001 - Enterprise IT Backbone Initialization

Field	Protocol Content
Objective	Verify that the WD-WM enterprise IT backbone loads governance protocols and verifies all eight ward stations before entering monitoring mode.
Method	Power-on test with normal, degraded, and missing-station conditions.
Acceptance Criteria	System enters monitoring only when required stations and governance services are available; otherwise enters fail-safe and records event.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-001.

VV-002 - WM-001/WM-003 Data Acquisition

Field	Protocol Content
Objective	Verify continuous acquisition of vital sign, LiDAR point-cloud, and thermal matrix streams.
Method	Run continuous acquisition across all bed stations; inject sensor disconnect and malformed frame conditions.
Acceptance Criteria	Valid data is accepted; invalid or missing frames are rejected or marked degraded without producing unvalidated clinical outputs.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-002.

VV-003 - WD115 Ambient Care Intelligence Classification

Field	Protocol Content
Objective	Verify that WD115 transforms raw sensing data into non-identifiable ambient care representations and applies data minimization.
Method	Feed identifiable-like, raw point-cloud, thermal, and minimal test vectors through WD115 pipeline.
Acceptance Criteria	Only ambient, non-identifiable, clinically purposeful representations are released downstream; suppressed records are logged.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-003.

VV-004 - Fall / Bed-Exit / High-Risk Event Detection

Field	Protocol Content
Objective	Verify detection of fall, bed-exit, high-risk posture, and spatial anomaly triggers.
Method	Use bench simulation and scripted ward scenarios across the 8-bed topology.
Acceptance Criteria	Detection performance meets predefined sensitivity, specificity, and latency targets; false alerts are characterized.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-004.

VV-005 - WD071 Constitutional Drift Verification

Field	Protocol Content
Objective	Verify drift scoring, threshold comparison, hardware interrupt generation, and Tier 2 escalation.
Method	Inject out-of-envelope inference outputs and altered model behavior.
Acceptance Criteria	Out-of-threshold drift triggers freeze or interrupt, blocks clinical output, notifies supervisor within configured window, and logs event.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-005.

VV-006 - WD116 Silent Elder Consent and Zero-Default Harm

Field	Protocol Content
Objective	Verify consent tier handling for direct consent, proxy appointment, and emergency necessity.
Method	Execute patient direct consent, proxy consent, expired proxy, revoked proxy, and emergency fallback cases.
Acceptance Criteria	Non-essential recommendations are blocked without valid consent path; emergency path requires configured

	justification and logging.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-006.

VV-007 - Sacred Pause Clinician Verification Delay

Field	Protocol Content
Objective	Verify mandatory delay prior to clinical output and accurate pause event logging.
Method	Measure delay duration under normal, high-load, and repeated-trigger scenarios.
Acceptance Criteria	No output is released before completion of configured pause; pause duration, trigger, and release state are logged.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-007.

VV-008 - WM-005 Biometric Unlock and Role Authorization

Field	Protocol Content
Objective	Verify iris/eye scanner authentication and clinician role authorization prior to sensitive output release.
Method	Test authorized clinician, unauthorized user, failed biometric, timeout, and lockout cases.
Acceptance Criteria	Only authorized clinician receives release token; failures are rejected, locked out per policy, and recorded in WD117 ledger.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-008.

VV-009 - Controlled Clinical Output Generation

Field	Protocol Content
Objective	Verify that output remains alert/recommendation/environmental support and does not autonomously initiate treatment.
Method	Execute allowed, rejected, and escalated output scenarios.
Acceptance Criteria	System output conforms to allow/reject/escalate logic; no clinical treatment action is executed autonomously.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-009.

VV-010 - WD117 Immutable Ledger Recording

Field	Protocol Content
Objective	Verify cryptographic recording of enforcement events, Sacred Pause delays, drift flags, biometric unlocks, and event traces.
Method	Generate representative events and attempt post-record modification.
Acceptance Criteria	Records include timestamp, event type, station, hash or equivalent integrity value, and are resistant to modification or deletion.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-010.

VV-011 - Regulatory Submission Data Packaging

Field	Protocol Content
Objective	Verify generation of HSA/FDA evidence packages from WD117 event records.
Method	Compile test data packages for simulated pre-market and V&V evidence submissions.
Acceptance Criteria	Package includes required event records, attestation summaries, exception logs, and traceability references.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-011.

VV-012 - Fail-Safe, Sovereign Brake, and Lockout

Field	Protocol Content
Objective	Verify safe-state transition when governance engine, authentication, sensor, or ledger functions fail.
Method	Induce governance service crash, ledger write failure, authentication failure, and sensor disconnect.
Acceptance Criteria	System transitions to safe state, suspends clinical output where required, notifies supervisor, and requires authorized reset.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-012.

VV-013 - 8-Bed Ward Topology Integration

Field	Protocol Content
Objective	Verify multi-station deployment and prevention of cross-bed routing errors.
Method	Run concurrent events at multiple bed stations with network and processing load.
Acceptance Criteria	Events remain associated with correct bed station; latency remains within defined limit; no cross-patient event mixing occurs.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-013.

VV-014 - Local Processing and Privacy Boundary

Field	Protocol Content
Objective	Verify no unintended cloud transmission, audio capture, camera capture, or unauthorized data export.
Method	Inspect hardware configuration, network traffic, logs, and interface permissions during operation.
Acceptance Criteria	No camera/audio streams are present; no cloud transmission occurs; exports require authorized workflow and are logged.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-014.

VV-015 - Human Factors and Clinician Workflow Validation

Field	Protocol Content
Objective	Verify that clinicians can identify alerts, complete Sacred Pause verification, use WM-005 authentication, and respond appropriately.
Method	Conduct simulated-use testing with representative caregivers/clinicians and critical tasks.
Acceptance Criteria	Critical tasks are completed without unacceptable use error; residual use risks are addressed by design or labeling.
Evidence Output	Test report, raw data/log extracts, deviation record if applicable, and traceability update for VV-015.

5. Test Evidence Checklist

Evidence Area	Expected Artifact
Bench/simulation evidence	Scenario scripts, raw detection logs, pass/fail summary
Software evidence	SRS, architecture, unit/integration/system test reports, traceability matrix
Risk evidence	Hazard analysis, risk control verification, residual risk evaluation
Human factors evidence	Task analysis, formative findings, summative validation report
Cyber/privacy evidence	Network isolation results, access control results, data minimization evidence
Regulatory packaging evidence	WD117 generated package, event logs, attestation report

6. Submission Positioning

For FDA/HSA use, the system is positioned as a monitored alert and governance platform.

> ***The system provides alerts, verification controls, and governance evidence to assist clinicians and caregivers; it does not independently initiate clinical treatment decisions.***