Claims:

5.1 Non-Device CDS Version – Methods and System Claims

- **System Claim – SmartStop Notification System:** *A clinical alert notification system* comprising: **(a)** a central server configured to receive real-time infusion pump alarms and clinical event notifications; **(b)** a nurse wearable device network (smartwatches or mobile devices) registered to multiple caregivers; **(c)** a proximity detection module using Bluetooth or equivalent technology to determine caregiver location relative to patient devices; and **(d)** notification software logic that, upon detection of a high-priority event, automatically selects a target caregiver based on proximity and alert priority and sends an electronic alert to that caregiver's wearable device, wherein the alert includes information about the event sufficient for the caregiver to understand the basis of the event and wherein the system requires the caregiver's acknowledgment input to record the alert as addressed. The system operates without adjusting any medical device parameters, serving solely to inform and prioritize caregiver response (thereby functioning as a Non-Device Clinical Decision Support tool).

- **Method Claim – Proximity-Based Alerting Method:** *A method of delivering a clinical alarm to a healthcare provider*, the method involving: **(i)** monitoring outputs from one or more medical devices or electronic health record systems for conditions that meet predefined critical criteria; **(ii)** when a condition is detected, identifying a nearest suitable clinician by evaluating signals from location or proximity beacons associated with clinicians and the location of the condition; **(iii)** transmitting an alert message to a wearable device of the identified clinician, the message comprising the patient identity, the nature of the alarm, and contextual data from the medical device or record; **(iv)** starting a timer upon sending the alert; **(v)** if an acknowledgment is received from the clinician's device within a first time threshold, marking the alert as acknowledged and stopping any further escalation; and **(vi)** if no acknowledgment is received within the first time threshold, automatically escalating the alert to an alternate provider or higher-tier responder and repeating the notification and timing steps. The method emphasizes human confirmation and does not initiate any automated clinical intervention beyond communications.

- **System Claim – Audit-Trail Enabled Alert Device:** *A clinical support system* wherein every alert and response is logged in a tamper-evident audit repository, comprising: a secure database or ledger that appends entries for each alert trigger, each notification dispatch, each user acknowledgment, and each escalation action, with timestamps and unique identifiers; wherein the system provides an interface for authorized personnel to review the sequence of events for each incident (for example, to answer "why did the pump alarm not get immediate attention" by showing the alert was sent at 14:32 and acknowledged at 14:35). This claim highlights the integration of an **immutable audit trail** with the alerting system[7].

- **Method Claim – Clinical Alert Acknowledgment and Logging:** *A method to record caregiver response to an electronic alert*, including: presenting an interactive prompt on a

caregiver's device for each alert that requires immediate attention; detecting a user input that acknowledges or responds to the alert; associating the input with the alert and halting any further redundant notifications for that event; and writing a log entry of the acknowledgment including caregiver ID, timestamp, and alert details to a secure audit log. Optionally, if the alert is not acknowledged, the method records the non-response and triggers higher-severity logging and escalation steps. This method ensures that **for every alert either an acknowledgment or a fail-safe action is documented**, facilitating compliance and post-event analysis.

- **System Claim – EHR-Integrated Alert Aggregator:** *A hospital integration system* comprising interfaces to both medical devices and electronic health records, wherein the system cross-references active device infusions with patient clinical data and generates caregiver alerts only when a relevant combination occurs. For example, if a patient's EHR data indicates a new contraindication (like an imaging contrast allergy noted while an infusion is running), the system cross-references the infusion drug and allergy list and sends an alert to the clinician, but without making any automatic changes to the infusion. This system claim underscores SmartStop's ability to combine device data and EHR context to create meaningful alerts while leaving decisions to humans.

5.2 Device-Integrated (510(k)) Version – Methods and System Claims

- **System Claim – SmartStop with Automated Safety Interlock:** *A dual-mode clinical monitoring and intervention system* comprising: **(a)** the elements of the notification system as described above (server, wearable alerts, proximity logic, etc.), and **(b)** a device control interface linked to an infusion pump or therapy delivery device, wherein the server is further configured to issue a command to temporarily suspend or adjust the therapy device's operation under predefined emergency conditions; wherein the emergency conditions include at least the combination of a continuing alarm state from the therapy device and a lack of human acknowledgment within a maximum safe response time; and wherein the system ensures that any such command is recorded and immediately communicated to clinical staff. This effectively claims the SmartStop system as an "extension" of the infusion pump that can autonomously prevent harm if clinicians fail to respond, thus an **infusion pump safety interlock mechanism**.

- **Method Claim – Escalation and Automated Pump Shutdown:** *A method for escalating unattended infusion alarms to an automated device action*, involving: **(i)** monitoring an infusion pump alarm state and concurrently sending alerts to designated clinical staff as per the earlier method; **(ii)** progressively expanding the circle of notified personnel (e.g., from assigned nurse to team lead to physician) if no acknowledgment is received, over a defined timeline; **(iii)** upon reaching a critical time without acknowledgment, sending a command to the infusion pump to execute a safety action (pause or stop infusion); **(iv)** receiving confirmation from the pump that the action is executed; and **(v)** after executing the command, generating a final alert to all relevant staff indicating the pump has been automatically stopped for safety. The method concludes with requiring a manual reset or input from a clinician at the pump before normal operation can resume. This method ensures a **closed-loop fail-safe response** to otherwise unmitigated alarms, combining communication and control.

- **System Claim – Infusion Pump Network with Central Override:** *A system of networked infusion pumps* in which each pump is communicatively connected to a central monitoring service (SmartStop), the central service capable of overriding a pump's operation under specific authorized conditions. The claim would specify that the pumps have a command API that the central service uses only when a safety rule is met (e.g., dosing about to exceed a 30-minute limit and no clinician present to intervene[10]). The novelty in such a system is the introduction of a **remote override capability** that is triggered not by the pump's internal programming alone but by a supervisory logic that accounts for caregiver non-response.

- **Method Claim – Verified Two-Channel Stop Command:** *A safety method for delivering a remote stop command to a medical device*, comprising: generating a stop signal from a primary logic engine when conditions are met; independently verifying the condition through a secondary channel or sensor (if available) to reduce false triggers; then transmitting the stop command over a secure channel to the device; and requiring an acknowledgment handshake from the device. If no acknowledgment is received (e.g., network failure), the method may include retrying or engaging a backup safety measure (like a page to a code team). This method is oriented to satisfy regulatory concerns that any remote command is robust and failsafe (for instance, using dual verification akin to how hardware watchdogs have dual timers[18]).

- **System Claim – Dual-Mode Clinical Support Apparatus:** *A clinical support apparatus operating in two modes – advisory and interventional*, wherein in a first mode it behaves as a non-device clinical decision support system (providing alerts and information to healthcare providers with no direct device control), and in a second mode (enabled via a regulatory-cleared configuration) it additionally provides device control signals to connected therapy equipment under emergency logic. This dual-mode design is such that the interventional features can be disabled or enabled based on regulatory authorization, allowing the same platform to be used initially as software-only and later as a combined software-hardware safety system. This claim essentially covers the design of SmartStop as an upgradable platform, which could be an important commercial and patent point – the idea that you can deploy it as just a notification system and later turn on the pump-stop capability via software update once approved, without hardware changes.

Additional

Non-Device CDS

claims

#	System claims (software-only embodiment)

S-1	A rules-driven priority-index generator that dynamically weights each alert by clinical severity, proximity score and caregiver workload, then routes to the highest-ranked clinician.
S-2	A role-mapping engine that cross-references hospital HR rosters so only credentialed staff (e.g., chemo-certified RNs) can receive specific drug alerts.
S-3	An offline-cache layer on the wearable that stores the last N alerts when Wi-Fi is lost and auto-syncs acknowledgements upon reconnection, preserving CDS status.
S-4	An adaptive-throttle module that suppresses repeat alerts if the same condition re-fires inside a programmable cool-down window, preventing alarm fatigue.
S-5	A compliance analytics dashboard that visualises median alert-to-acknowledge time by unit, staff role and shift, drawing data directly from the immutable ledger.

#	**Method claims**
M-1	Generating a composite priority score $P = \Sigma(\text{Severity}*w_1 + \text{Proximity}*w_2 + \text{Workload}*w_3)$ for every alert and routing to the clinician with the lowest P value.

M-2	Updating clinician availability by polling badge-reader sign-ins each minute and recalculating routing without interrupting pending alerts.
M-3	Auto-silencing subsequent alarms for a device when an initial alert is acknowledged and the underlying condition resolves within X seconds.
M-4	Persisting alert payloads in encrypted wearable storage when connectivity < -80 dBm and replaying acknowledgements once RSSI > -70 dBm.
M-5	Periodically hashing the last 1 000 ledger entries into a Merkle root and exporting it to a hospital SIEM for independent timestamp notarisation.

Additional

Device-Integrated (510 k)

claims

#	**System claims (pump-control embodiment)**
S-6	A redundant authorisation pathway that requires concurrence from both SmartStop logic and the pump's built-in safety CPU before executing a remote stop.

S-7	A predictive fail-safe simulator running on the server that models drug delivery 60 s ahead and flags impending overdoses before hard limits are breached.
S-8	A dual-network segmentation gateway isolating therapy-control traffic from hospital IT traffic, with a one-way data diode for status telemetry.
S-9	A hardware-watchdog handshake whereby the pump confirms stop execution within $T \leq 500$ ms or triggers a secondary hard-relay cut-off.
S-10	A remote supervisory override console allowing two-factor authenticated physicians to restart a halted pump after root-cause documentation.

#	**Method claims**
M-6	Deploying OTA rule-set updates cryptographically signed with FIPS-140-2 keys and activating them only after checksum verification by both server and pump.
M-7	Executing a dual-factor override whereby a bedside nurse scans a QR badge and an attending physician enters a PIN to restart therapy post stop-event.

M-8	Injecting a zero-volume “dry-run” command to the pump during low-acuity periods to verify network latency and watchdog responsiveness without affecting flow.
M-9	Rolling back an automatic stop if post-event data proves the alarm condition false, restoring the previous infusion rate while logging the rollback rationale.
M-10	Assigning hierarchical Escalation Severity Scores to concurrent alerts and prioritising automated stops only for the highest-scoring unresolved event per patient.