Description

Title

System and Method for Real-Time Smart Pump Bypass Detection and Intervention

Field of the Invention

This invention relates to infusion pump safety systems. In particular, it concerns systems and methods for detecting when a smart infusion pump's dose error reduction software (drug library) is bypassed and for providing real-time interventions to prevent medication errors.

Background

Smart infusion pumps with dose-error-reduction software (DERS) are widely used in healthcare to reduce intravenous medication errors. These pumps include drug libraries with predefined dose limits for medications. However, a caregiver can choose to operate the pump in a basic infusion mode (with "no drug selected"), bypassing the drug library safeguards. Bypassing DERS removes safety guardrails and is known to increase the risk of infusion errors, especially for high-alert medications such as potent vasopressors or opioids.

Existing infusion pump systems provide connectivity and data logging that can record or display when a pump is infusing in basic mode, but they generally do not actively intervene at the point of care. For example, current smart pump platforms (offered by vendors such as Becton Dickinson, B. Braun, Baxter, ICU Medical, Fresenius Kabi, etc.) can transmit pump status to a central server or dashboard. These systems allow retrospective analysis or real-time monitoring by remote staff, and may generate alerts for dose limit violations. However, there is no known commercial system that automatically detects a drug library bypass event on a high-risk medication and immediately notifies the caregiver with a dedicated alarm or forces corrective action in real time. Typically, if a nurse programs a pump in basic mode, the pump will display a generic warning (on-screen) that no drug library is selected, but it will not prevent the infusion or actively alert others. It remains up to hospital procedures and human vigilance to catch and correct such situations.

Therefore, a need exists for an improved infusion pump safety system that can detect in real time when an infusion is initiated or running outside of the prescribed safety software parameters (for example, without using an appropriate drug library profile) and that can actively intervene. Desired features include: identifying that a high-alert medication is being infused without safety limits; alerting the bedside clinician in a clear and urgent manner (e.g., audible or prominent visual alarm specific to this condition); notifying remote personnel (such as pharmacists or

supervisors) immediately; associating the event with the responsible user; escalating the alert if unaddressed; and optionally taking automated corrective action (such as pausing the infusion or guiding the pump to reprogram using the correct drug profile or order).

Moreover, it would be advantageous if such a system could cross-check the pump's programming against external data (e.g., the electronic health record (EHR) medication orders or the hospital's drug library) in real time. By comparing what is being infused to what was ordered or to known safe parameters, the system could infer the intended drug and dose, even if the pump is in basic mode, and catch discrepancies or omissions immediately. No current solution offers a fully automated real-time cross-verification between infusion pump settings and the prescribed orders to alert of a mismatch at the moment of infusion programming.

In summary, existing technology lacks the capability to automatically detect and respond to unsafe infusion pump programming (such as bypassing DERS on critical medications) at the time it occurs. The present invention addresses this gap by providing systems and methods for real-time smart pump bypass detection and coordinated intervention.

Summary of the Invention

The invention provides a system and method for real-time detection of drug library bypass events in infusion pumps and for automated intervention to enhance medication safety. In one aspect, the system comprises an infusion pump equipped with sensors and communication interfaces, and a monitoring module (which may be integrated into the pump or part of a networked server) that continuously monitors the pump's programming status and infusion parameters. The monitoring module is configured to determine when the pump is operating without an active drug library profile or otherwise outside of predefined safety limits for the medication. Upon detecting such a condition—especially if the medication is identified or inferred to be a high-alert drug—the system triggers one or more intervention responses in real time.

In various embodiments, the intervention responses include:

- **Bedside Alerting:** Generating an immediate alert at the point of care. This may involve an audible alarm (e.g., a distinct tone or spoken warning from a speaker on the pump) and/or a prominent visual notification on the pump's display to inform the caregiver that the infusion is not safeguarded by the drug library. The alert can present a message (for example, "Warning: High-risk medication – safety limits not active!") and may require the user to acknowledge the warning.

- **Automated Prompt or Lockout:** The system may prevent the infusion from proceeding until the issue is addressed or may require a confirmation or authentication. For instance, if a high-risk medication is being started in basic mode, the pump can automatically pause infusion and prompt the user to either select an appropriate drug library entry or enter a valid override code (such as a second clinician's confirmation or pharmacist authorization) before continuing. This acts as a forcing function to ensure deliberate review of the programming.

- **Remote Notification:** The system can send real-time electronic notifications to designated remote devices or personnel when a bypass event is detected. For example, a message can be pushed to a pharmacist's computer dashboard, a charge nurse's

smartphone, or a centralized monitoring station, indicating that a specific pump (identified by location or ID) is infusing a high-alert drug without DERS protection. The notification may include details such as patient, drug (if known or inferred), current rate, and time of event.

- **Escalation of Alerts:** If the unsafe condition is not corrected within a predetermined time frame, the system can escalate the alert. Escalation may involve increasing the urgency of the alarm (e.g., a louder or more persistent alarm at the pump), notifying higher-level personnel (such as the unit supervisor or rapid response team), or in extreme cases initiating automated safety measures (like gradually stopping the infusion if no action is taken and if it is safe to do so). Multiple tiers of alarms can ensure that the issue gets prompt attention.

- **User Attribution and Logging:** The system logs the event with a timestamp and, if available, the identity of the user who programmed or acknowledged the infusion. This can be achieved by capturing the user login on the pump or correlating with the electronic medical record (for example, linking to the nurse who documented the infusion start). Such attribution supports accountability and allows targeted training to reduce future bypass events. All details of the incident (pump ID, drug, rate, duration of bypass, acknowledgments, etc.) are recorded for quality improvement analysis.

- **Cross-Checking with Orders and Libraries:** In some embodiments, the system cross-references the infusion parameters with hospital data to ensure correctness. For example, the monitoring module can query the patient's active medication orders from an EHR system to find if there is a matching order for the infusion being administered. If a match is found (e.g., an order for Norepinephrine at a certain concentration and dose), the system can infer that the current basic infusion is likely that medication. The system can then alert the user that the infusion does not match the ordered protocol. In advanced embodiments, the pump can offer to automatically program itself according to the verified order (pulling the correct drug library entry and dose) with a single confirmation from the user. If no matching order is found, the system warns that the infusion may be unauthorized or misprogrammed. Additionally, the system can check the pump's parameters against the drug library limits: if the infusion rate exceeds any recommended limit for the inferred drug or care area, it will generate an immediate hard alarm and could prevent the infusion from running to avert an overdose.

The invention can be implemented in various forms. In one embodiment, all intelligence is built into the infusion pump device itself: the pump's onboard processor runs the monitoring and alerting algorithms, and the pump directly outputs local alarms and enforces safety prompts. In another embodiment, a networked approach is used: the infusion pump streams data to a central server or cloud platform which performs the monitoring analysis and coordinates alerts both at the bedside (by sending commands back to the pump to display alarms or pause the infusion) and to remote recipients. In yet another embodiment, a hybrid approach is employed wherein the pump handles immediate local detection and warning, while a connected hospital information system handles cross-checking with orders and broader notification escalations.

By covering these various configurations, the invention ensures that any attempt to administer a critical infusion outside of established safety processes is rapidly detected and addressed through

multiple feedback channels. This proactive safety net greatly reduces the likelihood of serious medication errors and encourages compliance with infusion programming best practices.

Brief Description of the Drawings

The accompanying drawings, which are incorporated in and form a part of this specification, illustrate embodiments of the invention and together with the description serve to explain principles of the invention:

- **FIG. 1A** illustrates an example smart infusion pump (100) with integrated safety monitoring components. The pump's housing and user interface (110) are shown, along with internal components such as a controller (120), a network communication interface (130), and an audible alarm speaker (108).
- **FIG. 1B** shows an exemplary display screen (110) of the infusion pump presenting a warning message (115) indicating that no drug library is selected for a high-alert medication infusion. The display also includes a prompt (116) for the user to confirm or correct the programming.
- **FIG. 2** is a schematic diagram of a networked infusion monitoring system according to an embodiment of the invention. It depicts multiple infusion pumps (100A, 100B) connected via a network (220) to a central monitoring server (200). The server is also interfaced with an electronic health record system (300) and with remote client devices such as a pharmacist station (230) and a clinician smartphone (232). Data flows and alert transmissions between these components are illustrated.
- **FIG. 3** is a flowchart illustrating a method of local real-time detection and intervention on an infusion pump. The process includes monitoring the pump's mode and parameters (step 302), detecting a library bypass condition (step 304), and triggering an on-pump alert and/or lockout sequence (steps 306–310) which requires user acknowledgment or reprogramming before infusion continues.
- **FIG. 4** is a flowchart illustrating a coordinated remote alert and escalation process. After detecting an unsafe infusion event (step 402), the system sends a notification to designated remote personnel or devices (step 404). If the situation is not resolved within a set interval (decision 406), the system escalates the alert level or notifies additional authorities (step 408), and may issue secondary actions such as reminding the bedside clinician or pausing the infusion (step 410).
- **FIG. 5A** shows a user interface prompt (500) on the pump's display that leverages EHR integration. In this example, the system has identified a matching medication order (502) for the ongoing basic infusion. The prompt (500) offers the user an option (504) to automatically reprogram the pump with the correct library entry and dose from that order, or alternatively an override option (506) if the user insists on proceeding.
- **FIG. 5B** shows an example of a remote notification on a mobile device (510) for a bypass alert. The alert message (512) indicates the patient, drug (inferred or entered manually), and the nature of the warning (e.g., "Library bypass on high-risk infusion").

The interface provides an acknowledgment button (514) for the recipient and may allow communication back to the pump or to other staff.

Detailed Description of Embodiments

The invention will now be described in detail with reference to the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings and the following description to refer to the same or like parts.

Embodiment 1: Pump-Integrated Detection and Alert

Referring to FIG. 1A, a smart infusion pump 100 is depicted according to one embodiment of the invention. The pump 100 includes a user interface 110 (which may be a touchscreen or a display with buttons) for programming infusions. Internally, the pump has a controller 120 (such as a microprocessor or microcontroller) and memory 122 that stores, among other things, a drug library database 124 containing entries for various medications with safe dosing parameters. The pump also has a communication interface 130 (e.g., a wireless network card or wired connection) enabling data exchange with external systems. In addition, the pump is equipped with an audible alarm device, such as a speaker 108, and may have visual indicators like indicator lights 109.

In normal operation, a clinician programs the pump 100 by selecting a drug from the drug library database 124 on the interface 110, which activates DERS for that infusion. The controller 120 checks the entered dose and rate against the library limits and issues alerts if they exceed soft limits or prevents entry beyond hard limits. However, the user also has the option to select a basic infusion mode (no drug profile). According to the invention, the controller 120 continuously monitors whether the current infusion is using a library profile or not. This status can be determined by the pump's software state (for example, a flag indicating "library mode" vs "basic mode") or by whether an active drug ID from the library is associated with the running program.

If the controller 120 detects that the pump is infusing in basic mode without an active drug profile, it will then evaluate additional context to determine if this situation warrants intervention. In one configuration, the pump simply treats any instance of bypass as a trigger for an alert. In a preferred configuration, the pump checks whether the medication being infused is known or likely to be a high-alert medication that should not be run without safeguards. This can be done in multiple ways: - The pump may prompt the user to input or select the drug name even in basic mode (for instance, the user might select "Norepinephrine" but choose not to use the pre-set concentrations or limits). If the user enters the drug's identity in some way (or scans a medication barcode), the pump can recognize that this is a high-risk drug. - Alternatively, the system can infer the drug by comparing the programmed infusion parameters to known standard concentrations or dose ranges. For example, if the pump is infusing at 5 mL/hour from a 250 mL bag labeled as containing 4 mg of a drug, the system might deduce the drug and concentration. - In another approach, the pump's connectivity (if available) can be used to query a hospital database or the EHR for any active orders for the patient that match the infusion (this approach is detailed further in Embodiment 2).

Once the system has determined that the pump is delivering a potentially high-alert medication without DERS, it initiates an immediate alert to the user. FIG. 1B shows an example of the

pump's display 110 presenting a warning message 115 in such a scenario. The message 115 may read, for instance, "**Warning: No Drug Library – High-Alert Med**" along with details like the current rate and a prompt 116 instructing the user to take action. In one embodiment, the pump will also emit a distinctive audible alarm via speaker 108. This alarm could be a voice output stating "Library bypass detected" or a unique tone that staff are trained to recognize as a DERS bypass alert. The use of an audible alert that specifically corresponds to this condition is novel, as conventional pumps typically only use generic alarms for technical issues or dose limit violations (which, in basic mode, are not available).

At this point, the pump 100 may also enforce a safety interlock. For example, the controller 120 can automatically pause the infusion when the alert is triggered, preventing further delivery of the medication until the issue is addressed. The user interface 110 might display options such as "Select Drug Profile" and "Override". If "Select Drug Profile" is chosen, the pump will guide the user to pick the appropriate drug from the library (or even automatically select it if it inferred the drug, as described later). If "Override" is chosen, the system may require a secondary confirmation, such as scanning a second nurse's badge or entering a one-time code provided by pharmacy, to proceed with the infusion in basic mode. This two-step confirmation for high-risk medication bypass adds a layer of accountability and deliberation, ensuring the decision is not taken lightly or by accident.

The pump's memory 122 records the event, including timestamp and details (and if user authentication is part of pump operation, it logs the user ID of the nurse who confirmed the override). By embedding the detection and at least initial intervention in the pump itself, Embodiment 1 provides a fail-safe that works even if the pump is not connected to any network. All actions happen locally and immediately.

To illustrate the process flow for this embodiment, FIG. 3 provides a flowchart. In step 302, the pump monitors infusion start or programming events. In step 304, a check is performed to determine if the infusion is being run without a drug library profile. If no (meaning a library is in use), normal safe operation continues (step 303). If yes, the logic moves to step 306, where the system determines if the infusion is high-risk (for example, by identifying the drug or recognizing the drug class or concentration). If the infusion is not considered high-risk (perhaps it's a routine fluid where library use is less critical), the system might simply log the bypass or present a gentle reminder. But if it is high-risk, the system proceeds to step 308 to trigger the alarm and alert displays as described. Step 310 then awaits user response: either the user confirms reprogramming with a proper drug entry, or confirms an override. If reprogrammed, the flow goes to step 312 where the infusion is restarted under the drug library safeguards (and the event is logged as resolved). If overridden, step 314 allows the infusion to continue in basic mode but marks the log with a confirmed override event; at this point the pump might also notify a remote system of the override (transition to Embodiment 2 functionality) if connectivity is available. The flow may also include a loop such that if the user takes no action for a certain time at step 310, the pump escalates the alarm (e.g., repeats it at higher volume or flashes the screen) to ensure it isn't ignored.

Through Embodiment 1, many immediate risks are mitigated at bedside: the nurse is clearly alerted that they are bypassing safety checks, and they are given an opportunity (indeed, a push) to correct the situation on the spot. However, this embodiment alone might rely on the presence

and diligence of the bedside nurse to react. The next embodiment extends the capability by involving networked resources and additional personnel for oversight.

Embodiment 2: Networked Monitoring, Notifications, and Cross-Checking

FIG. 2 illustrates an embodiment where the infusion pump 100 is part of a broader networked system that provides oversight and integration with other hospital systems. In this figure, two infusion pumps 100A and 100B are shown connected to a network 220 (such as a hospital Wi-Fi or LAN). A central monitoring server 200 receives data streams from these pumps (indicated by arrows from pumps to server). The server 200 may be a dedicated infusion safety server or a cloud service that aggregates real-time infusion data. The server has a monitoring module 210 that runs software algorithms to analyze incoming pump data for events of interest (including library bypass events as described). The server 200 is also interfaced with an electronic health record (EHR) system 300 which holds patient data and medication orders. Additionally, various client devices can connect to the server or receive alerts from it: for example, a pharmacy workstation 230, nurse central station, or mobile devices like smartphone 232 carried by clinicians.

In this embodiment, the infusion pump 100A still contains basic detection capability. The pump can transmit an event message to the server 200 as soon as it detects that it has started an infusion without a drug library entry or when a DERS limit is overridden. This message might contain the pump ID, the patient (if the pump is associated with a patient), the infusion parameters (rate, volume, perhaps an identifier of the drug if known or entered), and the nature of the event ("no drug selected" warning, override accepted, etc.). In parallel to any local alarm, sending this information to the server enables remote monitoring.

Upon receiving such an event (let's say Pump 100A is infusing in basic mode), the monitoring module 210 at the server side can initiate a cascade of responses: 1. The module 210 logs the event centrally and raises an alert in a dashboard interface that pharmacy or clinical engineering staff monitor. 2. The module cross-checks the infusion against the patient's medication orders in the EHR 300. This could involve looking up the patient's current IV medication orders. For instance, if Pump 100A is connected to patient John Doe and is infusing at 8 mL/h, and the EHR shows an active order for Norepinephrine 4 mg/250 mL for John Doe, the system infers Pump 100A is delivering Norepinephrine. It can then determine that this drug is classified as high-alert and that running it without DERS is a serious deviation. If the parameters or concentration used differ from the order (e.g., maybe the nurse entered a slightly different concentration manually), the system flags a mismatch. 3. The monitoring module 210 generates electronic notifications. For example, it may send a push notification to the charge nurse's smartphone 232 (FIG. 5B shows an example). The content of the notification 512 can include: "**ALERT:** Pump 100A (ICU Bed 5) running Norepinephrine without drug library. Rate 8 mL/h. Please check immediately." The message might appear in a mobile app or as a text alert. Similarly, a notification could pop up on the pharmacy workstation 230 or be sent via email/SMS according to hospital preference. The invention is not limited to a single communication method; it can integrate with existing alarm middleware to broadcast the alert to whoever is designated. 4. The system anticipates acknowledgment or corrective action. The alerted personnel can then intervene: for example, a pharmacist could call the nurse or send a message acknowledging the alert and advising on corrective steps. The nurse, upon being alerted on their device or by the pump's local alarm (from Embodiment 1), might then reprogram the pump properly. Ideally, the nurse will correct it,

and perhaps hit an "All Clear" button on the pump or remote app. 5. If no response is detected after a set time (as depicted in FIG. 4, decision 406), the system escalates. Escalation (step 408 in FIG. 4) could mean notifying a higher authority — e.g., the ICU manager or the hospital's patient safety officer — that a critical infusion is still running without safeguards. Escalation might also intensify the local alarm as mentioned. In certain embodiments, the system might be configured to send a command back to the pump to take further action (step 410). For example, after a prolonged disregard of the alert, the server 200 could remotely activate a louder alarm on the pump or flash its lights. In an extreme configuration, the server could issue a remote "pause" command to the pump 100A to temporarily halt the infusion (if it determines that continuing poses an imminent risk and that pausing is clinically safer than continuing). Typically, remote stop commands are used cautiously; the system could require two-authority approval (say, both the pharmacist and a physician) to remotely stop an infusion, which is then done in a controlled manner.

To support these actions, the pump 100 and server 200 share a secure communication protocol. The pump's network interface 130 may use standard hospital network encryption to send events. The server 200 could use vendor-specific APIs or an integration standard (like the IHE Patient Care Device messages) to interface with the pump. For example, in one embodiment the pump is an off-the-shelf smart pump that doesn't natively support remote pausing. In that case, the server might only be able to *request* the nurse to stop it via alerts rather than actually commanding the pump. In another embodiment, the pump firmware is designed to accept certain remote commands from trusted systems (for instance, as part of an interoperability solution with the EHR where start/stop can be controlled).

Another aspect of Embodiment 2 is the comprehensive logging and analytics. The server 200 aggregates these events from all pumps. It can produce real-time compliance dashboards showing, for each unit, how many infusions are running with the drug library enabled vs bypassed. It can track patterns, such as particular shifts or users that often bypass. Since the identity of the user who started the infusion can be obtained (either the pump can forward the user login info if the nurse logged into the pump, or the server can correlate the timing with who documented the med administration in the EHR), the system can automatically attribute each bypass event to a specific clinician. The system might generate periodic reports or even feed data into performance evaluations or additional training modules for those users, closing the loop for quality improvement.

The synergy between the pump and external data also enables the cross-checking feature in more depth. FIG. 5A depicts how a pump's interface might look when integrated with the EHR in the system. Suppose the nurse began a basic infusion, and the server identified a matching order for that drug. The server can send to the pump (or if the pump has direct EHR connectivity, it can retrieve) the details of that order. The pump's display 110 then shows prompt 500: "Order found: Norepinephrine 4 mg in 250 mL, start rate 8 mL/hr". The interface may provide a one-touch confirmation button 504 labeled, for example, "Apply Order Settings". If the nurse presses this, the pump automatically switches out of basic mode and loads the Norepinephrine library entry with the prescribed settings, effectively correcting the issue with minimal effort. Alternatively, if the infusion in progress had a slight discrepancy (maybe the nurse intended to titrate differently than the order initially), the system could allow them to adjust but still use the correct drug profile (ensuring at least the guardrails are in place). Optionally, an override option 506 might

still be present to proceed without applying the order, but again that could require secondary confirmation as described.

By implementing Embodiment 2, the safety net extends beyond the bedside to involve remote experts and automated cross-checks, greatly enhancing the chance of catching an error. It essentially creates a real-time infusion supervision system layered on top of existing smart pumps. Even if the bedside nurse misses the on-pump warning or proceeds anyway, the wider team and system are alerted and can respond.

It should be noted that the embodiments described can be combined in various ways. For instance, the standalone pump (Embodiment 1) could operate on its own in a smaller clinic without network infrastructure, providing local protection. In a larger hospital with network capability, that same pump can connect and become part of Embodiment 2's architecture, gaining the remote notification and EHR integration benefits. The claims that follow are intended to cover all such arrangements, from self-contained devices to distributed systems, where the core inventive concept is real-time detection of unsafe infusion pump programming and initiating timely interventions to prevent medication errors.

Addendum Specification Biometric Clinician-Authentication & Audit-Capture Layer

1. Overview

This addendum describes an optional **biometric authentication module** that may be incorporated into any of the infusion-pump embodiments (stand-alone or network-connected) previously disclosed. The module combines (i) **three-dimensional ("3-D") depth-sensing facial recognition** for rapid, touch-free user identification and (ii) a **concurrent 2-D RGB audit-camera frame** that is cryptographically bound to each safety-critical interaction (e.g., drug-library bypass, guard-rail override, pump-setting change). All biometric processing is performed locally in a tamper-resistant secure element; only match metadata, hashed audit artefacts, and policy-driven alert packets are transmitted off-pump.

2. Hardware Additions (FIG. 1–series may be annotated accordingly)

Ref. No.	Component	Description
150	**Structured-Light / ToF Depth Camera**	Projects an infrared dot-pattern or time-of-flight pulse to capture a sub-second depth map of the clinician's face.

152	**RGB Camera**	Captures a simultaneous colour frame for audit logging and secondary 2-D fallback matching.
154	**Secure Crypto Element**	Dedicated MCU/TPM that stores encrypted facial templates, executes matching, timestamps events, and digitally signs audit hashes.
156	**Status LED / Prompt Indicator**	Signals when the pump expects a face to be centred; flashes green on positive match, amber on retry/fail.

The cameras (150, 152) share a common cover-glass and are mounted above or alongside the primary UI display. The secure element (154) is soldered to the main PCB and isolated from the application processor via an authenticated SPI/I²C bus.

3. Software / Firmware Workflow

1. **Trigger Condition.**
   Any attempt to **(a)** unlock the pump interface, **(b)** start an infusion without an active drug-library profile, or **(c)**override a hard dose limit invokes the FaceAuth() routine.
2. **Capture & Match (≤ 500 ms).**
   - **Depth Frame** from 150 and **RGB frame** from 152 are buffered.
   - Secure element 154 extracts a feature vector and compares it against enrolled templates.
   - If match-score ≥ configurable threshold η (e.g., 97 %), the action proceeds. A soft threshold ν (e.g., 90 %) may permit a second attempt before failure.
3. **Failure & Time-out Policy.**
   - After N failed attempts or T seconds (site policy), the pump enters **biometric-lock mode**: infusion paused (if safe), GUI greyed, and a "Face Failed" packet is pushed to the monitoring server.
   - Remote supervisory release can be effected via dual authentication (e.g., charge-nurse badge + remote pharmacist approval).
4. **Audit Package Composition.**
   - RGB frame → SHA-256 hash → stored immutably in on-pump ledger;
   - Signed JSON packet {eventID, pumpID, userID*, timestamp, matchScore, hash} sent to server. Raw facial data are *never* transmitted.
5. **Remote Escalation (extends FIG. 4).**
   Decision 406 now branches on biometric success:
   - **Yes:** normal flow continues, no escalation.
   - **No:** step 408 escalates with "Biometric Failed" severity; step 410 may broadcast a high-priority page, flash the pump's alarm LEDs, or execute a remote-pause command.

4. Enrollment & Template Management

- Enrollment of authorised clinicians occurs **off-pump** (e.g., at a secure workstation) or **locally** via administrator mode plus dual-person verification.
- Templates are AES-GCM encrypted with a pump-unique symmetric key stored in 154.
- Revocation: deleting a user's credential zeroises the template, invalidating all future matches.

5. Privacy & Regulatory Compliance

- The system operates as a **data-minimisation architecture**: depth maps are discarded post-match; only salted hashes are retained.
- Audit frames are retained for a configurable retention window (e.g., 30 days) and automatically purged or anonymised per HIPAA/GDPR.
- The feature may be disabled via policy flag for jurisdictions where biometric capture is restricted; the pump then falls back to existing PIN/badge workflows.

6. Alternative Embodiments

- **Multi-Factor Mode:** combine face match with existing RFID badge tap or numeric PIN for dual-credential assurance.
- **Edge-Inference Variant:** offload face-matching to a hospital edge server equipped with an FPGA accelerator; pump streams encrypted depth data, receives signed match token.
- **Wearable Integration:** leverage clinician smartwatch proximity + face match for zero-touch unlock, reducing false-positive attempts when multiple staff are near the pump.

7. Advantages

1. **Sub-second authentication** that mirrors modern smartphone UX, reducing workflow friction.
2. **Positive user attribution** for every guard-rail bypass or infusion start, supporting quality-improvement analytics and staff training.
3. **Immutable, cryptographically signed audit trail** ties each facial frame to the event ledger, bolstering medico-legal defensibility.
4. **Remote escalation** allows pharmacy or supervisory staff to intervene immediately upon a biometric failure, tightening safety loops.