Claims

1. **A safety monitoring system for infusion pumps**, comprising:
2. at least one infusion pump device configured to deliver fluid medication to a patient, the infusion pump including a programmable controller and a drug library of predefined medication dosing parameters;
3. a monitoring module communicatively coupled to the infusion pump (either integrated within the pump or on an external computing system) and configured to monitor an operational status of the infusion pump;
4. an alert output device associated with the infusion pump, capable of conveying an alarm perceptible to a user;
5. wherein the programmable controller is configured to detect when the infusion pump is infusing medication without an active drug library profile or outside of said predefined medication dosing parameters, and upon detecting said condition, the monitoring module triggers the alert output device to generate a real-time alert to the user indicating that a safety bypass condition has occurred.

6. The system of claim 1, wherein the infusion pump is further configured to determine whether the medication being infused corresponds to a high-alert medication category, and the monitoring module triggers the real-time alert only if the medication is classified as high-alert or critical.

7. The system of claim 1, wherein the alert output device comprises an audible alarm unit on the infusion pump, and the real-time alert includes an audible warning signal distinct from standard pump alarms.

8. The system of claim 3, wherein the audible warning signal is a spoken message generated by the pump, informing the user that the infusion is not using the safety drug library.

9. The system of claim 1, wherein the infusion pump's alert output device further comprises the pump's display screen, and the real-time alert includes a visual message on the display screen warning that no drug library safeguards are active for the current infusion.

10. The system of claim 5, wherein the visual message on the display prompts the user to either select an appropriate drug library entry for the infusion or to confirm an override to proceed without the drug library.

11. The system of claim 1, wherein the infusion pump's controller is configured to automatically pause or inhibit the infusion upon detecting the safety bypass condition, and to resume infusion only after receiving a user confirmation acknowledging the alert or after reprogramming with a drug library entry.

12. The system of claim 7, wherein the infusion pump requires an authorization input from a second authorized person or a code in order to continue the infusion in basic mode for a high-risk medication, providing a dual confirmation mechanism.

13. The system of claim 1, further comprising a network communication interface in the infusion pump and a remote monitoring server, wherein:

14. the infusion pump transmits data indicative of its status and programming (including whether a drug library is in use and current infusion parameters) to the remote monitoring server; and
15. upon the monitoring module (on the remote server) detecting the safety bypass condition, the system sends an electronic notification alert to at least one remote device or user.

16. The system of claim 9, wherein the remote device is a mobile communication device associated with a second clinician or supervisor, and the electronic notification includes information identifying the infusion pump, the patient or location, and details of the bypass condition.

17. The system of claim 9, wherein the remote monitoring server is interfaced with an electronic health record (EHR) system containing medication orders for the patient, and the monitoring module is further configured to cross-check the infusion parameters of the infusion pump against the patient's active medication orders to determine if the infusion corresponds to an existing order.

18. The system of claim 11, wherein if a corresponding medication order is found in the EHR for the infusion being administered, the system automatically identifies the ordered drug and dose, and the infusion pump or the remote monitoring server generates a prompt offering to automatically reprogram the infusion pump according to the medication order's parameters and drug library profile.

19. The system of claim 11, wherein if no corresponding medication order is found for the infusion, the remote monitoring server triggers an escalated alert indicating a potential unauthorized or unverified infusion.

20. The system of claim 9, wherein the remote monitoring server maintains a log of all detected safety bypass events, including timestamps and the identities of users involved, and provides an escalation mechanism such that if a bypass alert is not acknowledged or resolved within a predetermined time, a secondary alert or alarm is issued.

21. The system of claim 14, wherein the secondary alert comprises at least one of:

22. escalating the audible alarm on the infusion pump to a higher volume or different tone,
23. sending additional notifications to a higher-tier authority or multiple recipients,
24. and transmitting a command to the infusion pump to adjust, slow, or pause the infusion for safety until manual verification is completed.

25. The system of claim 1, wherein the monitoring module utilizes machine learning or rule-based algorithms to infer an identity of the medication being infused when the drug library is bypassed, based on factors including infusion rate, solution concentration, patient data, and historical medication profiles, and uses the inferred identity to determine if the medication is high-risk or to retrieve relevant dosing limits.

26. **An infusion pump apparatus** comprising:

27. a pumping mechanism to deliver IV fluid to a patient;
28. a memory storing a drug library of medication dosing guidelines and storing program instructions;
29. a user interface for receiving infusion programming inputs from a user;
30. an alarm unit including at least one speaker or indicator;
31. a processor coupled to the memory, user interface, and alarm unit, wherein the processor is programmed by the instructions to:

    - o detect when the user has initiated or is running an infusion without selecting a drug entry from the drug library;
    - o in response to said detection, determine if the infusion corresponds to a predefined high-alert medication or if the infusion parameters exceed a safety threshold;
    - o and upon such determination, automatically activate the alarm unit to issue an alert and modify the user interface to display a warning and options for corrective action before allowing the infusion to continue.

32. The infusion pump apparatus of claim 17, wherein the processor is further programmed to prevent the infusion from starting or continuing until the user either selects a drug from the library for the infusion or provides a deliberate confirmation to proceed without the library, thereby integrating a forcing function against inadvertent bypass.

33. The infusion pump apparatus of claim 17, further comprising a network interface, wherein the processor is further programmed to send a notification message through the network interface to a remote system upon detecting the infusion without a drug library, the notification message including data about the infusion and the pump's status.

34. **A method for real-time safety intervention in an infusion pump system**, the method comprising:

35. monitoring an infusion pump's operation to identify when the pump is being operated in a basic infusion mode without utilizing a predefined drug library profile;
36. upon identifying such operation, automatically determining whether the infusion involves a high-risk medication or an unsafe parameter based on at least one of: the medication identity, the infusion dosage/rate, or hospital-defined rules;
37. immediately alerting the attending user at the infusion pump of the condition by presenting a warning message on the pump's interface and/or emitting an audible alarm;
38. requiring a responsive action from the attending user, the action including either confirming an override to continue without the drug library or reprogramming the pump to use an appropriate drug library entry;
39. if an override is confirmed, logging the event with timestamp (and user identity if available) for accountability;
40. transmitting, in parallel with the local alert, a notification of the condition to a remote monitoring system;
41. evaluating, at the remote monitoring system, patient data to cross-verify if the infusion matches an active physician order, and if so, providing the option to automatically adjust the pump settings to match the order;

42. and upon lack of timely corrective action by the attending user, escalating the alert by notifying additional personnel or triggering additional safety measures.

43. The method of claim 20, wherein the step of escalating the alert comprises sending a second alarm or notification to a supervisor after a preset time interval and optionally issuing a command to the infusion pump to temporarily pause the infusion until it is verified.

44. The method of claim 20, further comprising analyzing a plurality of infusion pump safety bypass events over time to identify patterns, and updating at least one of: the drug library, hospital policies, or the criteria for triggering alerts, based on said analysis to improve future compliance.

45. **A non-transitory computer-readable medium** storing program instructions which, when executed by one or more processors in an infusion pump safety monitoring system, cause the system to perform the steps of the method of any of claims 20 through 22.

46. **A networked infusion management system** for preventing infusion pump programming errors, comprising:

47. a plurality of smart infusion pumps, each pump configured to enforce drug library limits during infusions and to communicate its infusion status over a network;
48. a central server connected to the network, the server having a processor and monitoring software that receives the infusion status from each pump in real-time;
49. wherein the monitoring software detects any pump that is infusing without active enforcement of a drug library profile or in violation of predefined safety parameters, and in response:
    - o flags the pump as non-compliant on a central dashboard,
    - o sends an immediate electronic alert to designated personnel responsible for that pump's location,
    - o and logs the event with details including time, pump identification, and infusion parameters;
50. and wherein the central server is further configured to interface with a hospital electronic ordering system to validate whether the infusion corresponds to a recorded medical order, and to alert if it does not.

51. The networked infusion management system of claim 24, wherein the central server can transmit a control signal back to a flagged infusion pump to modify its operation, the control signal comprising at least one of: a command to display a specific alert message on the pump, a command to increase the priority of the pump's alarm, or a command to pause the infusion, wherein the execution of a pause command requires a condition that no acknowledgment was received from local staff within a safety time window.

52. The networked infusion management system of claim 24, wherein each smart infusion pump includes a scanner or interface to receive medication identification (such as a barcode on an IV bag) and if a user attempts to start an infusion in basic mode with a medication that has a corresponding drug library entry, the system automatically

recognizes the medication and prompts the user to use the drug library entry instead, thereby seamlessly integrating safety checks into the workflow.

53. The networked infusion management system of claim 24, wherein the designated personnel for alerts include at least a remote pharmacist and the unit's charge nurse, and the system provides an interface for those personnel to acknowledge the alert and document any intervention actions taken in response.

54. A medication-delivery system comprising:

(a) an infusion pump having a user interface and a plurality of drug-library safety profiles;

(b) a depth-sensing camera configured to capture a three-dimensional facial image of a user attempting to modify a pump parameter;

(c) a secure hardware enclave operative to compare the captured facial image with one or more stored biometric templates and to output a match confidence score; and

(d) control logic configured to inhibit execution of the pump parameter modification unless the match confidence score exceeds a predefined threshold, wherein the pump generates a signed audit record comprising a timestamp, the parameter modification, and a cryptographic hash of a contemporaneously captured two-dimensional facial frame.

55. The system of claim 54, wherein the audit record is transmitted to a remote monitoring server that escalates an alert if the parameter modification remains inhibited beyond a predetermined time interval.

56. The system of claim 54, wherein the depth-sensing camera employs structured-light projection and the two-dimensional facial frame is captured by an RGB imager co-located with the depth-sensing camera.

57. The system of claim 54, wherein, upon a facial-match confidence score falling below the predefined threshold, the control logic automatically prompts the user for **secondary authentication** selected from the group consisting of: (i) entry of a personal identification number (PIN); (ii) presentation of an RFID, NFC, or magnetic-stripe staff badge; or (iii) biometric fingerprint scan on an integrated or peripheral sensor.

58. The system of claim 57, wherein failure to satisfy the secondary authentication within a configurable timeout period causes the pump to transition into a **biometric-lock state** in which infusion flow is paused, pending remote supervisory release.

59. The system of claim 54, further comprising **template-revocation logic** that, upon receipt of a revocation command digitally signed by an authorised administrator, irrevocably deletes a selected biometric template from the secure hardware enclave, thereby preventing future facial matches for the corresponding user identity.

60. The system of claim 56, wherein the template-revocation logic generates a revocation audit record that is cryptographically linked to the event ledger and propagates the revocation to all network-connected pumps within the facility.

61. The system of claim 60, wherein the audit record comprising the two-dimensional facial frame is retained in secure storage for a retention period configurable between 7 days and 365 days, after which the frame is either (a) permanently deleted or (b) anonymised by irreversible pixelation, according to a facility retention policy.

62. The system of claim 61, wherein the retention policy is automatically overridden to **preserve** audit frames associated with events classified by the monitoring server as "critical medication-safety incidents."

63. The system of claim 54, wherein the control logic requires **dual-factor authentication** comprising a successful facial match and successful RFID badge tap before permitting changes to hard dose limits stored in the drug-library profile.

64. **T**he system of claim 63, wherein the facial match and badge tap must originate from **two distinct clinicians** (dual-sign-off) to enable override of an infusion programmed with a high-alert medication flag.

65. The system of claim 54, wherein the remote monitoring server is configured, upon detection of a biometric-lock event persisting beyond a supervisory time threshold, to transmit a **remote unlock workflow** that requires concurrence from both a pharmacist workstation and a unit charge-nurse mobile device before issuing a cryptographically signed unlock token to the pump.

66. The system of claim 65, wherein the unlock token is valid only for a single transaction and expires if not applied to the pump within a predetermined validity window.

67. The system of claim 54, wherein the secure hardware enclave periodically performs **template freshness validation** by requiring each enrolled clinician to re-authenticate at least once within a rolling 30-day window, automatically flagging dormant templates for administrator review.

68. The system of claim 54, wherein the audit record further includes a cryptographic nonce generated by the secure hardware enclave, the nonce being included in a Merkle-tree hash committed to the immutable ledger to enable external verification that the audit record has not been altered after initial storage.

69. The system of claim 54, wherein the facial-recognition module is operable in a **privacy-enhanced mode** in which the depth-map data are processed entirely within volatile enclave memory and purged immediately upon match completion, leaving only the signed match-score and audit hash in non-volatile storage.