Claims

1. **A system** for automatically onboarding and managing infusion pump devices, **comprising**:
   – an **edge gateway device** configured to be coupled to one or more infusion pumps and non-intrusively monitor data communications from the infusion pumps in real time, the edge gateway including a protocol detection module that automatically identifies a communication protocol and device identity of each infusion pump by sniffing data transmitted by the infusion pump without requiring manual configuration;
   – a **secure communication interface** (operable over MQTT or HTTP(S)) within the edge gateway device, configured to establish a authenticated connection to a remote server using token-based authentication credentials[6] and to transmit pump data and identification information to said remote server;
   – a **cloud-based server system** (remote server) programmed to receive data from the edge gateway device, maintain an inventory database of detected infusion pumps including, for each pump, at least its model, firmware version, communication protocol, and a drug-library identifier or checksum; and
   – a **compliance analysis module** executing on the cloud-based server system, the compliance analysis module automatically comparing the inventory data against one or more compliance rules or update criteria and identifying infusion pumps that are non-compliant or due for software/library updates, and in response generating a recommended upgrade plan prioritizing remediation of identified compliance gaps;
   wherein the system is configured such that the edge gateway device performs protocol-adaptive parsing to accommodate different infusion pump vendors and formats, and wherein the system logs critical events and device data in a cryptographically signed audit trail to ensure tamper-evident records of pump status and management actions[7].

2. **The system** of claim 1, **wherein** the protocol detection module comprises a library of protocol signatures and parsers for a plurality of known infusion pump communication protocols (including HL7 messaging formats and proprietary serial protocols), and is operable to iteratively attempt parsing incoming data against said signatures until a match is found, thereby determining the protocol and device type autonomously.

3. **The system** of claim 1, **wherein** the edge gateway device is configured as a passive **inline tap** or sniffer that duplicates infusion pump data without intercepting or delaying it, such that the infusion pump's primary data flow to clinical systems remains unaffected[8]; and **wherein** the edge gateway device includes a fail-safe bypass or relay mechanism that, in the event of gateway failure or power loss, automatically allows data from the infusion pump to continue to flow to its intended destination unimpeded.

4. **The system** of claim 1, **wherein** the secure communication interface uses a **token-based authentication** mechanism selected from the group consisting of: a JSON Web Token (JWT) carried in an MQTT CONNECT message, an OAuth2 access token used in an HTTP Authorization header, or a client TLS certificate, to authenticate the edge gateway to the cloud-based server, thereby preventing unauthorized devices from injecting or receiving infusion pump data[6].

5. **The system** of claim 1, **wherein** the cloud-based server system further comprises a **visual dashboard or user interface** that displays the live inventory of infusion pumps and highlights compliance status, and wherein the recommended upgrade plan generated by the compliance analysis module includes a sequence of actions (firmware updates, drug library updates, device replacements) grouped into stages with associated priorities or schedules for implementation.

6. **The system** of claim 1, **wherein** the cryptographically signed audit trail is implemented by hashing and signing each event or message (including at least pump connection events, data transmissions, detected compliance issues, and completed upgrade actions) using a secure hash algorithm and a private key or secret, and storing these signed records in an append-only ledger or blockchain such that any tampering or omission of events is detectable[7][17].

7. **The system** of claim 1, **wherein** the compliance analysis module's rules include at least: (i) a rule checking that each infusion pump's drug library version matches an approved version for its area of use, and flagging the pump if not (indicating a DERS compliance issue[4]), and (ii) a rule checking each pump's firmware or software version against a stored list of required or current versions (as per manufacturer or safety bulletin), and flagging pumps running outdated or vulnerable versions.

8. **A method** for plug-and-play onboarding of an infusion pump and automated compliance management, **comprising**:
(a) **passively monitoring** a data communication channel of an infusion pump via an edge gateway device, without interfering with the pump's normal data flow;
(b) **automatically detecting** a communication protocol used by the infusion pump by analyzing one or more initial data messages from the pump with a set of protocol signatures, including detecting whether the messages conform to an HL7 format or a proprietary format[2];
(c) in response to identifying the protocol, **extracting device-identifying information** from the messages, including at least the pump's model or type and its firmware or software version, using a parser corresponding to the detected protocol;
(d) **registering** the infusion pump in an inventory database by creating an entry that includes the extracted model, firmware version, and other attributes of the pump, wherein said registering is performed automatically by the edge gateway communicating with a central server once the device is identified (zero-touch onboarding);
(e) **securing communications** between the edge gateway and the central server by obtaining or generating an authentication token for the session and establishing an encrypted message stream (via MQTT or HTTPS) to transmit the pump's data and identity, such that the central server can trust the source of data[11];
(f) **updating** the inventory database in real time with ongoing data from the pump, including any change in the pump's status or configuration (for example, if a new drug library is loaded on the pump, updating a field in the inventory for that pump's library checksum);
(g) **evaluating compliance** of the infusion pump's configuration by automatically applying predefined rules to the inventory data, the rules checking for conditions that indicate non-compliance or need for update (including at least drug library currency and

firmware version level);
(h) if a compliance gap or needed update is identified for the infusion pump, **generating an alert or record** indicating the issue (such as "pump requires update") and incorporating this into an upgrade plan; and
(i) **formulating a remediation plan** that schedules or recommends one or more actions to bring the infusion pump into compliance, and upon execution or completion of each action, logging the outcome in a tamper-evident audit log.

9. **The method** of claim 8, **wherein** step (b) comprises employing an **adaptive parsing algorithm** that tests the incoming data against multiple protocol templates in succession until a valid parse is achieved, including recognizing HL7 v2 message headers if present[2], or otherwise matching binary/ASCII patterns unique to known infusion pump protocols, and wherein the method further comprises updating said protocol templates via a software update to the edge gateway to support new pump models as they become available.

10. **The method** of claim 8, **wherein** step (e) comprises the edge gateway authenticating to the central server using a **JWT token embedded in the MQTT CONNECT packet**, and wherein the method ensures that all data transmitted is encrypted with TLS such that patient or device data is protected in transit, and unauthorized network entities cannot read or alter the infusion pump data stream[11].

11. **The method** of claim 8, **wherein** step (h) further includes classifying the severity or priority of the compliance gap based on policy – for example, a pump lacking the current drug library is classified as high priority due to dosing error risk[4] – and wherein the method triggers an immediate notification to responsible personnel if the priority exceeds a threshold (e.g., if an infusion pump is found to be running with DERS disabled or an expired library, a real-time alert is sent).

12. **The method** of claim 8, **wherein** step (i) comprises generating a **staged upgrade plan** covering multiple infusion pumps, including the pump identified in step (a) and any others with similar compliance issues, the plan grouping updates in phases to minimize clinical disruption (such as updating a limited number of pumps at a time while others remain in service), and further comprising adjusting the plan dynamically if some pumps are unavailable (e.g., in use by patients) so that the upgrades occur when feasible.

13. **The method** of claim 8, **further comprising** recording each significant event or action in a secure audit trail by computing a cryptographic hash of event data and appending it to an audit log with a digital signature, **wherein** the events recorded include at least: detection of a new device, data messages received from the pump (optionally in summary form), compliance flags raised for the device, and any manual overrides or confirmations entered by users; and **wherein** the audit trail is stored in a manner that is tamper-evident and auditable (for example, on a blockchain ledger or write-once medium)[7].

14. **An edge gateway apparatus** for infusion pump integration, **comprising**:
– one or more **hardware interfaces** to connect to infusion pump data ports, including at least a network interface port and/or a serial port, the hardware interfaces configured to tap into data transmissions from the infusion pump without disrupting them;

– a **microprocessor** and associated memory configured with program instructions that implement:
– a **sniffing module** that listens to incoming data on the hardware interfaces and buffers the data;
– a **protocol identification module** that analyzes the buffered data to detect a protocol signature and selects a corresponding data parser, thereby automatically determining a pump's communication protocol and message format;
– a **data extraction module** that, using the selected parser, extracts device-specific information from the data, including at least an identifier for the pump and version information; and
– an **edge client communication module** that establishes secure connectivity to a remote management server, including means for authenticating using a token or certificate and means for transmitting the extracted device information and subsequent pump data to the remote server;
– a **non-volatile storage** on the apparatus for caching data and event logs in case of network unavailability, such that no data is lost and can be forwarded when connectivity resumes; and
– a **fail-safe circuit** that, in normal operation, allows the microprocessor to intercept and copy data packets, but upon detection of a failure condition (power loss, watchdog timeout, or command), automatically bridges the infusion pump's connection through to the original destination to maintain continuous data flow.

15. **The edge gateway apparatus** of claim 14, **wherein** the protocol identification module is configured with a plurality of **pluggable parser components**, each corresponding to a different infusion pump protocol, and the apparatus further comprises an update mechanism to receive new or updated parser components (e.g., via a firmware update or plugin download), enabling the apparatus to support new infusion pump models without hardware modification (adaptive extensibility for future protocols).

16. **The edge gateway apparatus** of claim 14, **wherein** the edge client communication module publishes pump data to a cloud message broker using the MQTT protocol with Quality of Service guarantees, and wherein the module includes an internal **token store** or cryptographic module that securely stores authentication tokens or keys used to sign outgoing messages, thereby ensuring all outbound data streams are authenticated and encrypted.

17. **The edge gateway apparatus** of claim 14, **further comprising** a **local alert mechanism** (such as LEDs or a buzzer) controlled by the microprocessor, wherein the program instructions cause the apparatus to activate the local alert mechanism if a critical condition is detected in the sniffed pump data (for example, an infusion pump alarm indicating a serious error), thereby providing immediate localized notification in addition to remote reporting.

18. **A cloud-based infusion pump management server** (or server system), **comprising**:
– a **communications interface** configured to accept incoming data connections from one or more edge gateway devices as defined in claim 14, over secure protocols (TLS-encrypted MQTT, HTTPS, or similar);

– a **database** for storing an inventory of infusion pumps, including fields for device identity, model, firmware version, software/library details, and status;
– a **server processor** and memory containing program code that implements:
– a **data ingest module** that receives and normalizes data from the edge gateways, updating the database in real time as new pump records are received or existing records change;
– a **compliance rule engine** that accesses a library of compliance criteria and checks the inventory database against these criteria on a continual or periodic basis, identifying any infusion pump entries that violate a rule (signaling non-compliance or needing maintenance);
– an **upgrade planning module** that, responsive to the compliance rule engine, generates an optimized plan for bringing the infusion pump inventory into compliance, the plan including grouping of devices and scheduling of recommended actions, and outputs the plan via a user interface or notification system; and
– an **audit log module** that records events related to device data and compliance checks, including timestamps and cryptographic verifications, into an immutable log store;
– **wherein** the server is configured to provide user access (with appropriate security roles) to view the inventory status and approve or modify recommended upgrade actions via a graphical user interface or API.

19. **The cloud-based infusion pump management server** of claim 18, **wherein** the compliance rule engine's library includes rules based on at least one of: manufacturer-recommended firmware levels for each pump model, a schedule for drug library updates (e.g., requiring updates every 6 months), and safety alerts from regulatory agencies (such that if an agency issues a recall or alert for a certain device or software, the rule engine will flag all matching devices in the inventory).

20. **The cloud-based infusion pump management server** of claim 18, **wherein** the upgrade planning module uses a **priority weighting** for each compliance issue (taking into account factors like potential patient harm, frequency of use of the device, and regulatory urgency) to sort recommended actions, and automatically **batches similar actions** together – for example, scheduling all pumps of a given model that need a firmware update to be updated in the same maintenance window – and further **provides an output report** that includes a timeline and the list of devices for each batch.

21. **The cloud-based infusion pump management server** of claim 18, **wherein** the audit log module is interfaced with a blockchain or distributed ledger network, and for each event it generates a hash or transaction that is submitted to the ledger such that an external entity (e.g., an auditor or manufacturer node) can independently verify the sequence and integrity of logged events[16].

22. **A non-transitory computer-readable medium** storing program instructions which, when executed by one or more processors of a system comprising an edge gateway device and a cloud server, cause the system to perform the steps of the method of claim 8, including automatically detecting infusion pump attributes via data sniffing, securely communicating with a cloud inventory server, and analyzing compliance and upgrade needs for the infusion pump.

[1] [2] [3] [9] FRESENIUS_LIVRE-BLANC_interoperability-2023(17).indd

https://www.fresenius-kabi.com/content/dam/fresenius-kabi/global/documents/others/infusion-systems-and-interoperability-in-healthcare-systems.pdf.coredownload.inline.pdf

[4] [5] Case Study: Quality Improvement Strategy to Enhance Compliance with Dose Error Reduction Software: Focus on Hematology/Oncology

https://www.bainbridgehealth.com/resources/case-study-quality-improvement-strategy-to-enhance-compliance-with-dose-error-reduction-software-focus-on-hematology/oncology

[6] [11] A Deep Dive into Token-Based Authentication and OAuth 2.0 in MQTT | EMQ

https://www.emqx.com/en/blog/a-deep-dive-into-token-based-authentication-and-oauth-2-0-in-mqtt

[7] ProvisionalHierarchyDOCX.docx

file://file-So4BMfLVffY8Pwwxdqtu7o

[8] [13] [16] [17] [18] TRACELOOP OO NEW.docx

file://file-KYjTKHC5fQnnLSfNS42yUo

[10] [12] [14] [15] SmartStop_Sentinel_Connect™_Hospital_Wide_Sentinel_Event_Automation.pdf

file://file_00000000272c71f5aff1dfeadb9c5b45