Claims

1. A comprehensive credentialing and privileging system, comprising:

a. a skills-currency ledger module configured to automatically record practitioners' activities and accomplishments as verifiable micro-credentials, wherein the module receives data from clinical log sources including EHRs and networked medical devices and generates digitally signed credential records for each logged skill or procedure;

b. a predictive privileging AI module that analyzes credential data and external data to predict a risk score or outcome likelihood for each practitioner, the module providing proactive risk indicators used to inform or modify the granting of clinical privileges;

c. a biometric attestation subsystem enabling in-person supervision or task completion to be confirmed via biometric authentication, the subsystem capturing cryptographically signed confirmations from supervisors and practitioners (using biometric or FIDO2-based credentials) and associating those confirmations with specific credential events;

d. a smart-contract engine managing conditional privilege rules, wherein each grant of a privilege is encoded with conditions selected from time validity, required training or experience, and compliance statuses, and the engine automatically triggers modification or revocation of the privilege when the conditions are not satisfied;

e. a regulatory update scanner employing natural language processing to monitor and identify new or changed regulations or accreditation standards, and upon detection, automatically generating corresponding credentialing tasks or requirements within the system;

f. an integration interface for workforce management, providing API or plugin means for scheduling and resource allocation systems to query credential validity in real-time, thereby preventing assignment of personnel to roles for which credentials or privileges are expired or inadequate;

g. a device integration module that communicates with connected medical devices and training systems, receiving usage or performance data and issuing competency tokens or credentials based on device-specific proficiency criteria, thereby linking equipment usage with credential maintenance; and

h. a zero-knowledge proof module for sanction and compliance checks, configured to verify attributes such as "no active sanctions for the practitioner" via cryptographic proof (non-membership in a revocation list) without disclosing sensitive underlying data,

wherein all modules interoperably share data through a secure distributed ledger and identity framework such that credentials are tamper-evident, portable as W3C Verifiable

Credentials, and automatically enforceable across different institutions and systems.

2. The system of claim 1, wherein the skills-currency ledger module utilizes a permissioned blockchain network to store or anchor credentials, and each micro-credential entry is modeled as a token or ledger record that includes metadata about the procedure or skill, a timestamp, an issuer signature, and a reference to evidence (such as a supervisor attestation or device log), thereby providing an immutable audit trail of a practitioner's accumulated experience.

3. The system of claim 1, wherein the predictive privileging AI module comprises a machine learning model trained on historical practitioner profiles and outcomes, including malpractice claim history, patient outcome statistics, peer review data, and continuing education records, and wherein the module updates each practitioner's risk assessment continuously by incorporating new ledger entries and external alerts (such as national database queries), outputting alerts or recommendations (for example, suggesting denial of new privileges or additional monitoring) for high-risk practitioners.

4. The system of claim 1, wherein the biometric attestation subsystem uses FIDO2 WebAuthn standards to perform user verification and signature, such that when a supervised procedure is being logged, the system sends a challenge to a supervisor's registered authenticator device and to the practitioner's device, obtains signed responses that confirm their presence and approval, and encapsulates these responses into a verifiable credential of supervision stored in the ledger .

5. The system of claim 1, wherein the smart-contract engine is implemented on a blockchain smart contract platform and encodes conditions including: (i) time-bound expiration – the privilege credential includes an expiration date or block height after which it is inactive unless renewed; (ii) event triggers – hooks that listen for specific events such as completion of a required course or a threshold number of procedures on the skills ledger, and upon receiving cryptographic proof of such events, automatically update the privilege status; and (iii) revocation triggers – integration with the AI module and sanction check such that if a practitioner is flagged by AI or a sanction proof fails, the smart contract can suspend or revoke the relevant privilege credential immediately.

6. The system of claim 1, wherein the regulatory update scanner comprises a text ingestion pipeline and a large language model (LLM) tuned to recognize obligations in regulatory text, and further wherein the system maintains a mapping of regulatory topics to credential items so that when a new rule is detected (for example, a new mandatory training or a change in license renewal frequency), the system either automatically creates a new credential requirement entry for affected practitioners or adjusts existing credential parameters, with a citation or link to the source of the rule for audit purposes.

7. The system of claim 1, wherein the integration interface for workforce management provides a RESTful API endpoint that given an identifier of a practitioner and a

prospective role or procedure and date, returns a structured response indicating compliance or listing unmet credential items; the interface may also push webhook notifications to scheduling software whenever a practitioner's credential status changes (such as a certification expiring or being reinstated), thereby keeping external systems in sync with credential status in near real-time.

8. The system of claim 1, wherein the device integration module supports multiple device communication protocols (including IoT standards) to receive training and usage data, and wherein for a particular class of device it defines competency criteria – for example, for an infusion pump device, the criteria might be "complete manufacturer online tutorial" and "perform 5 supervised uses without error" – and upon detection that a user meets the criteria via data from the device (and any supervisor attestations if needed), the module issues a verifiable competency credential (optionally co-signed by the device manufacturer or hospital) that can be used to satisfy privilege requirements related to that device.

9. The system of claim 1, wherein the zero-knowledge proof module uses a cryptographic accumulator to represent a set of disqualified or sanctioned identities, and each practitioner's identity (license number or other ID) can be checked by requiring the practitioner (or a trusted authority on their behalf) to produce a non-membership proof with respect to the accumulator ; the system verifies this proof to determine if the practitioner's ID is absent from the sanction list, and if the proof is valid, the practitioner is treated as having "no sanctions," whereas if invalid or if membership is proven, the system triggers a flag or requests detailed review of that practitioner.

10. A method of credentialing and privileging professionals using a system as in claim 1, comprising:

(i) continuously collecting data on professional activities, outcomes, and requirements from disparate sources (electronic records, devices, regulatory feeds);

(ii) issuing digital micro-credentials and macro-credentials based on the collected data, each credential being cryptographically signed by an issuing authority and stored or referenced on a tamper-resistant ledger;

(iii) evaluating, via an AI algorithm, the risk profile of each professional by comparing their credential data and history to learned patterns associated with future adverse events or performance issues;

(iv) enforcing credential conditions automatically by using smart contracts or programmed business rules that update credential status when predetermined conditions (time elapsed, insufficient activity, lack of compliance) occur;

(v) validating critical credentialing events (such as supervised trainings or competency

demonstrations) with multi-factor authentication, including biometric factors to ensure authenticity of the participants;

(vi) responding to external rule changes by automatically modifying the set of required credentials or issuing alerts/tasks to professionals so they can meet new compliance obligations; and

(vii) integrating the credential validity information into operational systems like scheduling, such that no professional is assigned or allowed to perform a task unless their current verified credentials meet the requirements of that task,

whereby the method achieves a self-updating, self-auditing credentialing process that reduces manual effort, improves response time to risk and regulatory changes, and enhances trust through verifiability and privacy safeguards.

Cross-Reference to Prior Art Findings: The applicant has conducted a patent search and identified several references related to aspects of the invention. Notably, Axuall's U.S. Patent No. 12,079,891discloses foundational elements of a digital credential network with primary-source verification, which the present system builds upon by adding predictive analytics and smart privilege enforcement. Microsoft's U.S. Patent 9,768,962 B2 teaches zero-knowledge verification of credential status (non-revocation proofs), a technique incorporated in the invention's sanction check feature. WIPO Publication WO2020/192342 demonstrates a blockchain-based method for validating practitioner qualifications via authorized nodes, illustrating the feasibility of decentralized trust in credentialing, which is extended in this invention to a fuller feature set. Additionally, industry solutions by Medallion, Evercred , CertifyOS, and Silversheet have informed the background; however, those primarily address automation and digitization of existing processes, whereas the present invention provides an integrated, intelligent system with novel components (like AI-driven privileging and biometric verification) not found in combination in the prior art. These references are hereby incorporated by reference for their teachings where applicable, and the invention as claimed distinctly combines and enhances such teachings to achieve a new, comprehensive technical solution to credentialing challenges.