

From Paper Documents to Digital Trust

Securing healthcare credentials in the age of AI to drive longitudinal career mobility

A solution brief from
TruMerit® | Credivera®

Published: June 2026



TruMerit™
Global careers. Care anywhere.



From Documents to Digital Trust

Securing healthcare credentials in the age of AI to drive longitudinal career mobility

Published by
TruMerit® and Credivera®

© 2026 TruMerit. All rights reserved.

This publication may be shared for educational and noncommercial purposes with proper attribution to TruMerit. No part of this publication may be reproduced, distributed, or transmitted for commercial purposes without prior written permission from TruMerit. View our republication and reuse policy at trumerit.org.

Suggested citation

TruMerit and Credivera. (2026). "From Documents to Digital Trust: Securing healthcare credentials in the age of AI to drive longitudinal career mobility." TruMerit, 2026.

The information in this white paper is provided for informational and educational purposes only. It is intended to support discussion and awareness of emerging risks related to artificial intelligence, nursing credential fraud, workforce mobility, and credential verification, and to provide a solution framework for addressing this ecosystem. It does not constitute legal, regulatory, cybersecurity, immigration, clinical, or professional advice.

For more information

TruMerit.org
media@trumerit.org

Published: June 2026



Executive summary

Healthcare credentialing is entering a period of structural risk. Artificial intelligence is dramatically lowering the cost, skill, and time required to fabricate convincing professional credentials, identities, and employment histories. Fraud that once required manual effort can now be generated at scale—often with a level of sophistication that challenges traditional review processes.ⁱ

This shift is no longer theoretical. Research indicates that 85% of identity fraud cases now involve generative AI, demonstrating that AI is already central to how modern fraud is executed.ⁱⁱ At the same time, projections suggest that by 2028, one in four candidate profiles globally could be fake, underscoring the increasing difficulty of validating identity and qualifications in a digital-first environment.ⁱⁱⁱ

While artificial intelligence is accelerating the scale and sophistication of credential fraud, it is not the root cause. Credential fraud has existed for decades and continues to occur through more traditional means. Individuals may submit falsified diplomas, altered transcripts, counterfeit licenses, or misrepresented employment histories, often exploiting gaps in verification processes rather than relying on advanced technology. In many cases, these efforts do not require sophisticated tools, only the opportunity to operate within systems that depend heavily on document review and manual validation.

These traditional forms of fraud are particularly difficult to detect in high-volume environments, where credentialing teams are managing large applicant pools under time pressure. Inconsistent recordkeeping, fragmented international data systems, and reliance on email or phone-based verification can create delays or blind spots that fraudulent actors exploit. Even well-resourced organizations may struggle to confirm the authenticity of documents issued across different jurisdictions, especially when institutional records are incomplete, difficult to access, or not standardized.

Healthcare systems face this evolving threat while also managing growing workforce shortages and increasing cross-border mobility. Credentialing bodies must evaluate more candidates more quickly and across more complex regulatory environments—without compromising trust or safety.

Incremental improvements to existing verification processes are no longer sufficient. Instead, the healthcare ecosystem must transition toward a secure, interoperable digital credential architecture—one in which trust is not inferred from documents but proven through cryptographically verifiable credentials.

A verifiable digital credential ecosystem addresses these challenges at a foundational level. By replacing static documents with cryptographically secured credentials issued directly by trusted authorities, it becomes extremely difficult to falsify or manipulate credential data. At the issuer level, credentials are created as tamper-proof records tied to the issuing organization. At the verifier level, authenticity can be confirmed instantly and directly, without relying on document interpretation or manual outreach.

This closes the gap that has historically enabled paper-based and document-driven fraud, making it significantly harder for individuals to misrepresent qualifications—whether through traditional methods or more advanced techniques. This shift requires both trusted credentialing authorities and an enabling digital infrastructure.

Together, TruMerit and Credivera are advancing this model—combining global credential authority with secure digital credential technology to strengthen how trust is issued, maintained, and verified across the healthcare workforce.



The changing risk landscape: AI and credential fraud

Artificial intelligence is reshaping how credential fraud is created, executed, and scaled. Today, widely accessible generative AI tools allow individuals and organized actors to produce highly realistic credentials, application materials, and identity artifacts with minimal effort.^{iv}

These tools enable:

- High-quality forged diplomas and certifications.
- Fabricated employment histories and clinical experience.
- Replication of institutional logos, seals, and signatures.
- Rapid scaling of fraud attempts across jurisdictions.

This represents a fundamental shift. Credential fraud is no longer primarily manual or detectably inconsistent. It is increasingly automated, scalable, and difficult to identify through traditional means.

External data reinforces the magnitude of this shift. Organizations are already experiencing its impact—41% report having hired and onboarded a fraudulent candidate, indicating that identity verification systems are under significant strain.^v In healthcare, the stakes are especially high. Credential fraud is not merely an administrative or compliance risk—it creates direct exposure to patient safety issues and undermines trust across regulatory systems.^{vi}



“We are no longer verifying documents—we are being asked to validate identities, qualifications, and trust itself in an environment where AI can fabricate all three.”

Why legacy credentialing models are breaking down

Traditional credentialing systems rely on documents as representations of trust. That model is increasingly insufficient.

1. **Documents are no longer reliable indicators of authenticity.** Digital transformation has improved efficiency but not trust. In fact, digital document forgeries now account for 57% of all document fraud, surpassing physical counterfeits for the first time and increasing significantly in recent years.^{vii}
2. **Verification is slow and resource-intensive.** Many credential verification workflows still depend on manual processes—emails, phone calls, and document reviews. These approaches are difficult to scale and misaligned with the speed and volume required in modern workforce environments.^{viii}
3. **Global fragmentation creates gaps.** Cross-border credentialing introduces inconsistent standards, incomplete data access, and varying regulatory expectations. These factors create vulnerabilities that can be exploited by fraudulent actors.^{ix}
4. **Failures are already occurring at scale.** The prevalence of fraudulent hiring outcomes demonstrates that current verification models are not keeping pace with evolving risks.^x

Taken together, these weaknesses highlight a structural issue: the system continues to rely on artifacts that can be manipulated, rather than on mechanisms that can reliably prove authenticity.

From documents to verifiable digital credentials

Addressing these challenges requires a shift from document validation to proof validation.

A verifiable digital credential is:

- Issued by a trusted authority.
- Cryptographically secured.
- Held by the individual.
- Instantly verifiable by authorized third parties.

Unlike traditional credentials, these records:

- Cannot be altered without detection.
- Reflect real-time validity (including expiration or revocation).
- Enable direct verification without manual processes.

In this model, a fraudulent or invalid credential simply fails verification.^{xi}



"A document can be copied. A credential can be claimed. But a cryptographically verifiable record can only be proven."

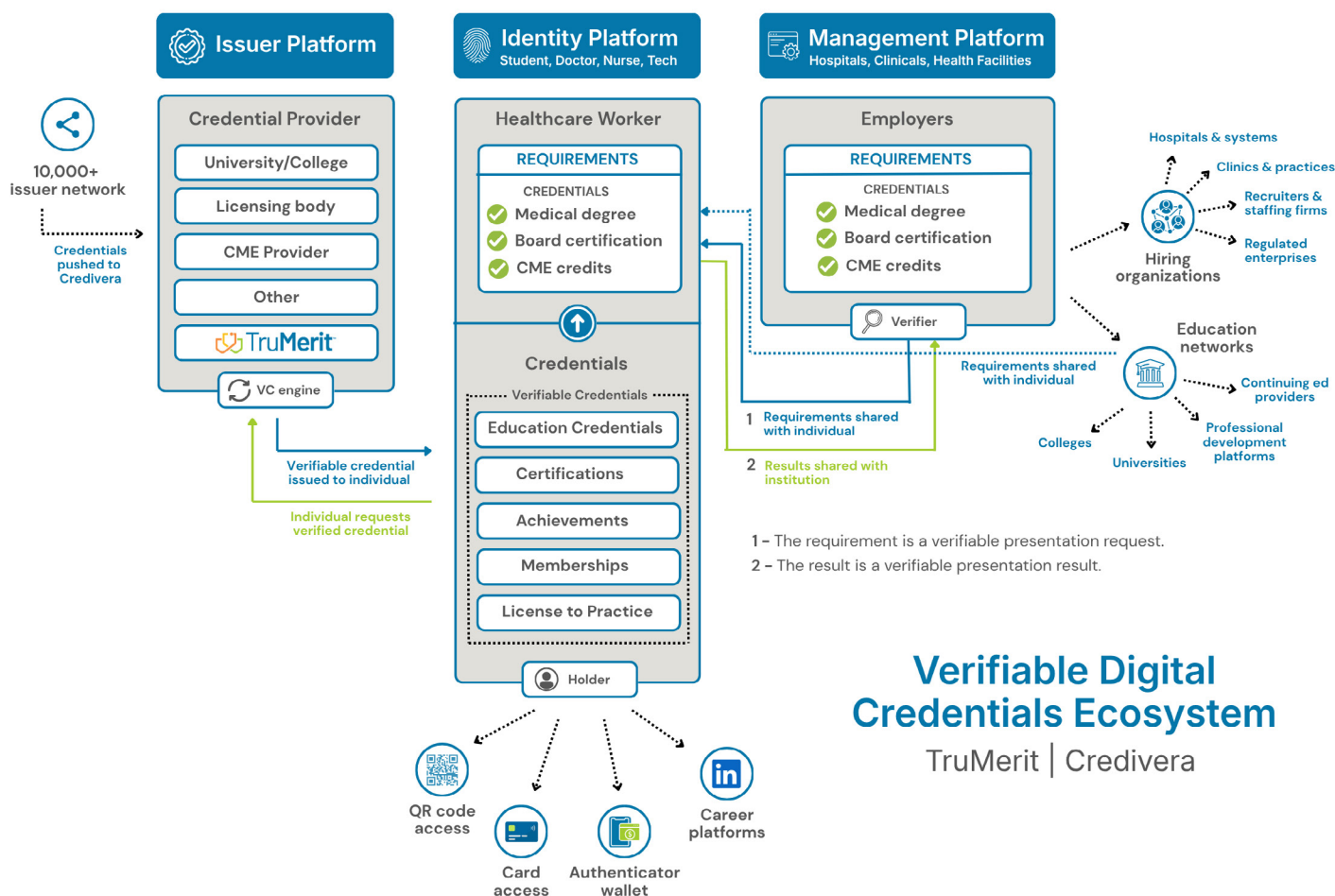




The verifiable digital credentials architecture

A verifiable credential ecosystem is built around three core roles:

- 1. Issuer**
Trusted organizations—such as credentialing bodies—issue credentials and maintain control over their lifecycle.
- 2. Holder**
Healthcare professionals securely store credentials and control how they are shared.
- 3. Verifier**
Employers, regulators, and other institutions validate credentials instantly, without the need for manual outreach.





This model aligns with global policy direction. For example, the European Union is implementing a digital identity framework that enables secure credential storage and exchange through standardized digital identity wallets.^{xii} These developments signal a broader shift toward interoperable, secure, and user-controlled identity systems.

Why does this matter?

A verifiable credential ecosystem delivers measurable advantages:

- **Fraud resistance:** Credentials cryptographically protected against tampering.
- **Real-time verification:** Reduction in delays and elimination of manual validation steps.
- **Issuer control:** Preservation of the authority and integrity of credentialing bodies.
- **Global portability:** Support for cross-border workforce mobility.
- **User empowerment:** Professionals empowered to manage and share credentials securely.





Operationalizing digital trust

A joint approach

Building a verifiable credential ecosystem requires both credential authority and digital infrastructure. TruMerit and Credivera bring complementary capabilities that enable this model.





TruMerit: Trusted credential authority

- Defines credentialing standards and evaluation processes
- Issues recognized certifications for healthcare professionals
- Maintains authority over credential lifecycle (issuance, revocation, expiration)
- Serves as a trusted source for regulators, employers, and governments

TruMerit operates at the center of global healthcare workforce trust. Its certifications, evaluations, and mobility services enable healthcare professionals, especially internationally educated nurses, to safely and efficiently enter regulated healthcare systems worldwide. As healthcare labor shortages intensify, cross-border workforce movement accelerates, and credential fraud risks increase, TruMerit faces mounting pressure to deliver faster, more secure, and more transparent credential verification on a global scale.

TruMerit's mission depends on trust. Employers, regulators, and governments rely on TruMerit to ensure that healthcare professionals are qualified, compliant, and job-ready. However, traditional credentialing models strain under modern realities:

1. **Rising global mobility:** Professionals frequently move across employers, jurisdictions, and countries.
2. **Operational friction:** Manual verification, paper documents, emails, and audits slow hiring and deployment.
3. **Fraud escalation:** Sophisticated fake credentials and AI-generated documents undermine confidence.
4. **Regulatory pressure:** Verification integrity is directly tied to patient safety and public trust.
5. **Candidate expectations:** Applicants expect digital-first, instant, and portable proof of qualification.

To remain authoritative while scaling globally, TruMerit requires a system that preserves issuer control, strengthens verification integrity, and improves experience for all stakeholders.



Credivera: Digital credential infrastructure

- Provides secure digital credential issuance technology
- Enables cryptographic signing and authentication
- Supports real-time credential validation
- Enables interoperability across systems and jurisdictions
- Provides secure digital wallets for credential storage and sharing

In this, Credivera functions as TruMerit's digital trust infrastructure partner—not replacing TruMerit's certification authority or evaluation processes, but instead, Credivera digitally extends them.

Credivera enables TruMerit to issue verifiable digital credentials as cryptographically secure representations of TruMerit-issued certifications and services; give professionals self-custodied control through digital wallets while TruMerit retains issuer authority to revoke, suspend, or update credentials; enable instant, real-time verification by employers, regulators, schools, and governments; and participate in a global digital credential ecosystem built on open, interoperable standards.

The result is a modern trust layer that travels with the worker and scales with TruMerit's mission.

Together, these capabilities create a system in which:

- Trust is anchored in recognized institutional authority.
- Credentials are secure and verifiable by design.
- Fraud risk is significantly reduced.
- Verification is faster and more scalable.
- Workforce mobility is improved.

This is not a replacement for existing credentialing systems—it is an evolution that extends trust into a digital, interoperable framework.



How it works

Building a verifiable credential ecosystem requires both credential authority and digital infrastructure. TruMerit and Credivera bring complementary capabilities that enable this model.

1.

Issuer-controlled digital trust.

Credivera ensures TruMerit remains the source of truth.

- TruMerit controls eligibility, issuance, revocation, and expiration.
- Credentials are cryptographically bound to TruMerit as issuer.
- Verification proves authenticity without exposing unnecessary personal data.

This preserves TruMerit's authority while eliminating dependence on paper, PDFs, or manual lookup.

2.

Dramatically faster verification cycles.

Credivera converts verification from a process measured in days or weeks to one that happens in seconds.

- Employers and regulators can instantly confirm credential validity.
- Expiration status and updates are verified in real time.
- Manual calls, emails, and audits are reduced or eliminated.

For TruMerit, this accelerates workforce deployment and reduces administrative burden without lowering standards.

3.

Fraud reduction and credential integrity.

Healthcare credential fraud presents a direct risk to patient safety and public confidence.

Verifiable credentials:

- Are tamper-proof and cryptographically signed.
- Cannot be altered, copied, or forged like PDFs or paper.
- Expose AI-generated or manipulated documents as invalid.

This materially strengthens TruMerit's role in safeguarding the public good and protecting quality care delivery.

4.

Global portability without re-verification.

Healthcare professionals increasingly require credentials that move with them. Credivera enables TruMerit-issued credentials to:

- Be reused across employers, jurisdictions, and borders.
- Align with emerging global digital identity standards.
- Support international hiring and regulatory workflows.

This positions TruMerit as a global enabler of workforce mobility, not a regional bottleneck.

5.

Improved applicant experience and trust.

From the applicant's perspective, Credivera transforms credentials into career assets. Professionals can:

- Access credentials permanently in a digital wallet.
- Share verified proof via QR codes or secure links.
- Showcase credentials in job applications and online profiles.

For TruMerit, this increases brand value, applicant satisfaction, and program differentiation.



A roadmap of high-value use cases

Global certification programs

TruMerit currently issues digital credentials to all global certification applicants who successfully pass applicable exams and meet the requirements for credential eligibility. This establishes a global, verifiable reputation for TruMerit certifications.

Immigration-support programs

TruMerit will issue its healthcare worker certifications (VisaScreen®), as required by United States Customs and Immigration Services (USCIS), as a verifiable digital credential on the Credivera network to support a fraud-free posture for credentials verification in support of healthcare workers seeking eligibility to practice or pursue education in the U.S.

Employer and regulator verification

Hospitals, staffing agencies, and regulators verify TruMerit credentials without having to contact TruMerit directly. This reduces verification backlog, improves hiring speed, and lowers the risk of credential misuse.

Career-long credential portfolios

Professionals accumulate multiple TruMerit-issued credentials and services over time. Credivera enables TruMerit to deliver a unified, longitudinal record of trust.

Digital badging with verifiable depth

While digital badges provide visibility, Credivera-backed credentials provide proof. Badges promote achievements; verifiable credentials validate them. This keeps TruMerit differentiated from marketing-only credential models.

Foundation for future digital identity services

Credivera positions TruMerit to expand into digital identity-supported migration workflows, continuous compliance monitoring, and cross-border regulatory alignment. The platform is not a point solution; it is infrastructure.

This model enables TruMerit to issue trust *once* and have it recognized everywhere. Together, TruMerit and Credivera modernize credentialing for a global healthcare workforce that demands speed, security, and certainty. This partnership allows TruMerit to scale its mission, reinforce its authority, and lead the transition from paper-based verification to digital trust.

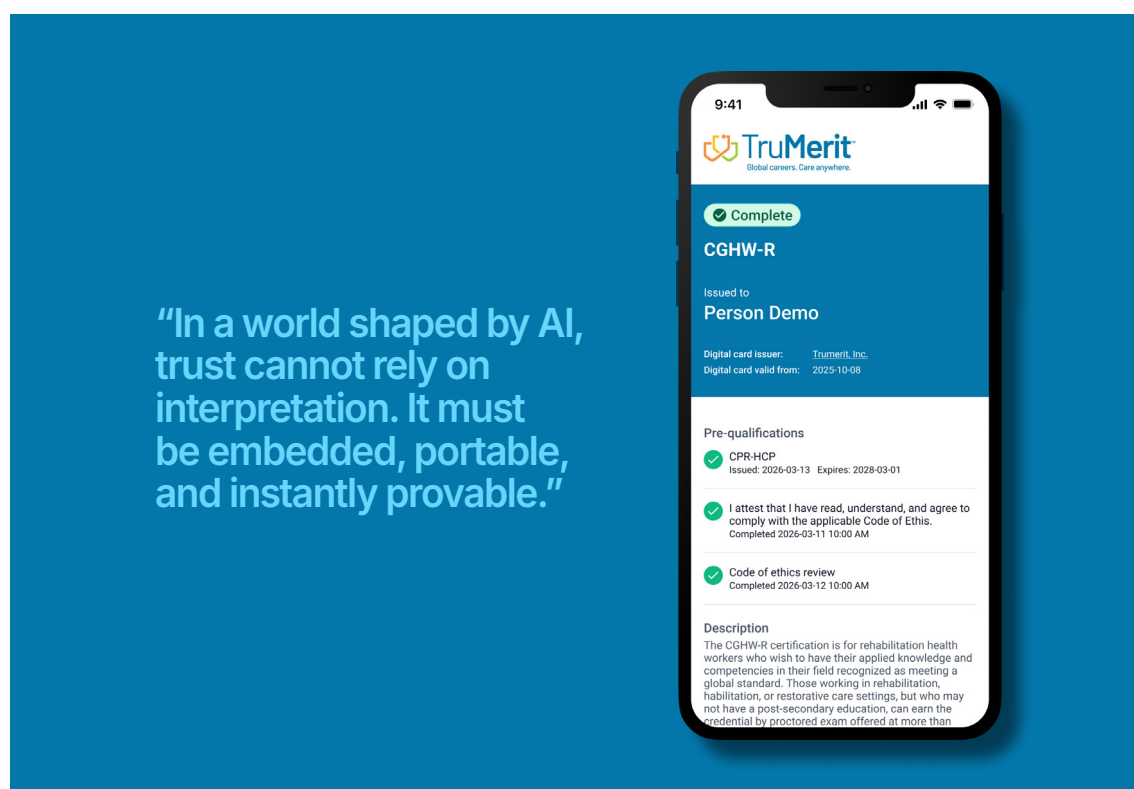


Conclusion: A structural shift in trust

AI-driven credential fraud represents a fundamental shift in the risk landscape. Traditional document-based verification methods are increasingly inadequate in a world where credentials and identities can be fabricated at scale.^{xiii}

Verifiable digital credentials offer a structural solution—embedding trust directly into credentials and enabling real-time validation across systems and stakeholders.^{xiv}

Through a combination of trusted credential authority and secure digital infrastructure, TruMerit and Credivera are working together to establish a more resilient, scalable, and future-ready approach to healthcare credentialing.



Learn more

Information about TruMerit's digital verifiable credentials services can be found here.
<https://www.trumerit.org/verifiable-digital-credentials/>



References

ⁱHerckis, L., Tse, E., & Grady, D. (2026). AI is supercharging nursing credential fraud: What you need to know. TruMerit.

ⁱⁱLexisNexis Risk Solutions. (2026). Global state of fraud and identity report.

ⁱⁱⁱCrist, C. (2025, August 8). By 2028, one in four candidate profiles will be fake, Gartner predicts. HR Dive.

^{iv}Herckis, L., Tse, E., & Grady, D. (2026)

^vGetReal Security. (2025, December 11). Deepfake readiness benchmark report.

^{vi}Herckis, L., Tse, E., & Grady, D. (2026)

^{vii}Entrust. (2024, November 19). Deepfake attempts occur every five minutes amid 244% surge in digital document forgeries.

^{viii}Herckis, L., Tse, E., & Grady, D. (2026)

^{ix}Herckis, L., Tse, E., & Grady, D. (2026)

^xGetReal Security. (2025, December 11)

^{xi}Herckis, L., Tse, E., & Grady, D. (2026)

^{xii}European Commission. (2026). European digital identity framework.

^{xiii}GetReal Security. (2025, December 11)

^{xiv}Herckis, L., Tse, E., & Grady, D. (2026)