AI is Supercharging Nursing Credential Fraud

What you need to know

A threat landscape briefing

Published by:
Global Health Workforce Development Institute

June 2026

TruMerit™
Global careers. Care anywhere.

AI is Supercharging Nursing Credential Fraud: What You Need to Know

A threat landscape briefing

Authors

Lauren Herckis, PhD
Senior Director, Center for Global Research and Policy, TruMerit

Emily Tse, MPhil
Senior Director, Global Affairs, TruMerit

David Grady
Cybersecurity and AI Specialist

Published by TruMerit®

Suggested citation
Herckis, L., Tse, E., & Grady, D. (2026). "AI is supercharging nursing credential fraud: What you need to know. A threat landscape briefing." TruMerit.

The content 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. It does not constitute legal, regulatory, cybersecurity, immigration, clinical, or professional advice.

For more information
TruMerit.org
media@trumerit.org

Executive summary

AI is rapidly transforming healthcare and fraud at the same time. While AI already powers breakthroughs in diagnostics, drug discovery, and operations, it is also lowering the barrier for bad actors to fabricate convincing nursing credentials and identities at scale. Fraud that once required time, skill, and manual effort can now be generated in minutes with off-the-shelf tools, making it easier for unqualified or fictitious providers to slip into critical roles and compromise patient safety.

Nursing credential fraud is particularly high stakes: nurses constitute a large share of the global health workforce and deliver most hands-on care. The combination of global nurse shortages, cross-border migration, uneven data standards, and increasingly sophisticated AI tools create a fertile environment for AI-enabled credential fraud. Traditional, largely manual verification methods are no longer sufficient on their own.

This paper argues that AI-driven credential fraud should be seen as a strategic risk, not a back-office compliance issue. It recommends several priority responses: build AI fluency across regulators, credential evaluators, and employers so they can use AI defensively and understand its limitations; strengthen collaboration and information-sharing among regulators, professional bodies, employers, credentialing organizations, and law enforcement; and invest in secure digital identity and verifiable credential infrastructures that make tampering harder and verification faster.

Why read this paper?

This paper is designed to help you understand how artificial intelligence (AI) makes nursing credential fraud easier to perpetrate and harder to detect. It also frames the case for increased research into this emerging threat and calls for more coordination among stakeholders to build the awareness, tools, policies, and competencies needed to turn the tables on AI fraudsters.

No matter your role—Chief Nursing Officer, HR credentialing manager, State Nursing Board leader or regulator—you can become a powerful ally in the fight against AI-powered nursing credential fraud.

Action starts with awareness.

Introduction: Suddenly, AI is everywhere.

For many of us, artificial intelligence (AI) seems to have appeared out of nowhere in just the last year or two, suddenly integrated into our professional and personal lives at almost every turn. Mainstream use of AI exploded with the public release of ChatGPT in late 2022, but computer scientists and software engineers have, in fact, toiled for decades to build the underlying data models that make AI so powerful. The roots of modern AI go back to the mid-1950s; today, AI is routinely hailed as one of the most transformative technologies in human history.

AI has begun to reshape almost every aspect of healthcare, from research and drug development to imaging, diagnostics, and the end-to-end patient experience. At the same time, however, individuals and well-resourced organized crime groups are taking healthcare fraud to a whole new level with the help of AI. For example, the U.S. Department of Justice (DOJ) recently uncovered a $700 million scheme in which Medicare beneficiaries' identification numbers and other confidential health information were allegedly obtained through theft and deceptive marketing. "The defendants allegedly used artificial intelligence to create fake recordings of Medicare beneficiaries purportedly consenting to receive certain products," according to the DOJ.[i]

AI-fueled healthcare fraud has the potential to go far beyond reimbursement scams, because AI enables motivated individuals to cheaply and easily create sophisticated fraudulent credentials. This allows would-be providers to fabricate details about their education, their certifications, and even their true identities, often with extraordinary precision.

The emerging threat of nursing credential fraud is particularly problematic given that nurses make up nearly half of the healthcare workforce globally and provide nearly 80 percent of hands-on care.[ii] AI's ability to accelerate credential fraud in healthcare creates obvious perils, from threats to patient health and safety to reputational, legal, and financial exposure, and even regulatory punishment.

But AI can be a powerful force for good, too. In 2025, the U.S. Department of Justice announced a new Health Care Fraud Data Fusion Center that uses AI, cloud computing, and advanced analytics to spot reimbursement fraud schemes and anomalous billing patterns.

These tools can and should be used to augment human expertise in the fight against nursing credential fraud.

Credential fraud before AI

Nursing credential fraud is not a new phenomenon. Long before AI entered the picture, regulators, employers, and credentialing organizations encountered individuals who misrepresented or fabricated their education, licenses, and work histories to gain access to nursing roles. Typical schemes involved forged diplomas, altered transcripts, counterfeit licenses, borrowed or stolen license numbers, and inflated or invented job titles. Until recently, these abuses were enabled by the sheer volume of paper-based records that had to be authenticated by hand. The challenge of verification is compounded by the huge number of nurses seeking employment outside their home country, as international data standards and recordkeeping systems vary widely from region to region.

In the pre-AI era, most nursing credential fraud was highly manual and relatively "low tech." Creating a fake diploma or transcript required time, basic design skills, and access to printing or document-editing tools.

Bad actors often relied on crude cut-and-paste jobs, typewritten alterations, or low-resolution reproductions that could sometimes be spotted by a careful reviewer.

The verification of submitted credentials was an equally manual and arduous process. Human resources, medical staff services, and credentialing teams often depended on phone calls, mailed forms, and faxed confirmations to validate education and licensure. In this environment, fraudulent nurses sometimes slipped through simply because reviewing staff were overloaded, documentation was inconsistent, and no one had the time or tools to connect the dots.

When credential fraud *is* discovered, it creates shockwaves across the healthcare community. The most recent high-profile example is the ongoing "Operation Nightingale" investigation, in which several for-profit Florida nursing schools sold more than 7,000 fraudulent nursing diplomas and transcripts that were then used to obtain licensure and work as nurses across the U.S. This scheme—unaided by AI as it allegedly began in 2019—was highly effective until patterns emerged that raised suspicion and led to a federal investigation and many criminal charges. But it took investigators years to crack that case, and it likely would have been even more successful had today's powerful Gen AI tools been available at the time.

"In the pre-AI era, most nursing credential fraud was highly manual and relatively 'low tech.' Now, with AI, the level of sophistication employed in credential fraud has grown exponentially."

Credential fraud in the AI era

A global health worker shortage and shifting trends in nurse migration compound the critical need to maintain integrity, reliability, and rigor in credential verification of nursing professionals. However, the rise of off-the-shelf AI tools with extraordinary capabilities (see sidebar) gives impostors a way to automate and scale nearly every step of the credential fraud process.

With AI tools, individuals and professional fraudsters alike can produce polished resumes, cover letters, and application narratives that map directly to a specific job description or institutional expectations. They can generate plausible descriptions of clinical rotations, continuing education, and prior roles, complete with appropriate terminology and local context. Institutional logos, signatures, watermarks, and seals can be reproduced or approximated with a level of professional polish that would once have required specialized tools and expertise. In fact, AI enables online "template farms" where the user can choose from thousands of fake credentials and identify documents from around the world. With a simple point, click, and the addition of a headshot and other customizations to the template, online fraud becomes a turnkey self-service.

Further, bad actors can "spoof" email addresses to make it appear they are writing from a legitimate educational institute. These synthetic documents are often good enough to survive casual visual inspection and basic digital checks. And AI is increasingly being used to create "deepfakes," which are real-time voice and video conversations that present very convincing illusions of people who do not

exist or who are impersonated. Deepfakes can be exceedingly difficult to identify; ZeroFox, a cyber security company, reported in 2025 that deepfake content has become so realistic that 99.9% of consumers in the U.S. and UK are unable to identify fake content without specialized tools.[iii]

A 2025 Gartner study estimates that by 2028, 1 in 4 job candidate profiles will be fabricated by AI.[iv] In its most recent report, the Association of Certified Fraud Examiners (ACFE) detailed occupational fraud cases in 138 countries and reported healthcare as among the industries reporting the most fraud cases.[v]

It seems that all the elements and conditions needed for widespread AI-enabled nursing credential fraud are in place.

AI tools: A primer

Powerful and easily accessible AI tools have moved from research labs into the browser windows and phone screens of everyday users. Today, most people encounter AI through conversational "chatbots" like OpenAI's ChatGPT, Anthropic's Claude, and Google's Gemini, but these products sit on top of underlying "large language models" (LLMs) that do the real work.

Other commercially popular platforms build on similar technology, including Microsoft Copilot, image-first tools like Adobe Firefly, and many industry-specific assistants are embedded inside Electronic Health Record (EHR) systems and office productivity software suites.

Generative AI vs. agentic AI

Most of today's widely used tools are forms of Generative AI, which are systems that create new content—text, images, code, audio—based on a user's prompt. "GenAI" is fundamentally reactive: you ask for a draft discharge summary, a prior-authorization appeal, or a patient handout, and it produces that specific artifact.

Typical GenAI capabilities include:

- Text creation and refinement: Drafting emails, policies, clinical summaries, patient education materials, and marketing copy; rewriting for different audiences and tones.
- Ideation and iteration: Generating lists of ideas, outlining presentations or white papers, and iterating on drafts with rapid "what if we tried this instead?" cycles.
- Code generation: Writing code inspired by natural language queries, translating between programming languages, and allowing the rapid development of fake websites and "template farms."
- Photorealistic image generation: Creating realistic or stylized images, including headshots, from text prompts.
- Multimodal input and output: Increasingly, AI models can accept text, images, audio, or files as input and analyze them in tandem (for example, "reading" clinical images and interpreting data from a chart).

Agentic AI goes a step further. Agentic systems can plan and execute multi-step tasks toward a goal with less human hands-on involvement. Instead of simply drafting a letter, agentic AI can automate the submission and follow-up of fraudulent job applications, essentially operating independently.

Preventing the next wave

Recommendations for collaborative action

How can the healthcare community turn the tables on AI-driven fraud? As the world's largest credentials verification and evaluation body for nursing and allied health professions, continue reading to see recommendations offered by TruMerit.

1. Foster "AI fluency" and close the "guidance gap."

Many nursing regulators, credential evaluators, and other verification stakeholders are starting to use commercial AI tools, but AI fluency—being able not just to use these tools, but to understand their limits, interpret their outputs, and integrate them thoughtfully into existing workflows—is still largely missing, and most professionals are left to figure it out on their own.

TruMerit recently conducted a comprehensive review of academic literature, professional journals, and other sources to measure if and how those involved in credential review currently understand the threat of AI-driven nursing credential fraud, and if best practices are emerging and being shared. They found that although awareness of AI's many legitimate uses in healthcare delivery is expanding, a major gap persists in awareness and formal education around AI's role in perpetuating and combating nursing credential fraud.

Many interested parties, from clinicians and academics to law enforcement professionals, are increasingly sharing anecdotes, case studies, and informal best-practice recommendations in professional forums and online discussions. But more formal, evidence-based scientific study about the use of AI in licensure credential fraud is needed.

A "guidance gap" also exists. Much has been written in the mainstream press about "AI and the future of healthcare," but formal regulatory guidance specifically addressing AI's use as an anti-fraud tool is hard to find, if it exists at all. The United States National Council of State Nursing Boards (NCSBN), for example, recommends using AI to augment human decision-making. UNESCO has released "Recommendation on the Ethics of Artificial Intelligence,"[vi] and a number of studies about the general application of AI in health care have appeared in professional and scholarly publications and in podium presentations at various industry conferences.

TruMerit recommends that regulators continue to update best practice guides and toolkits on fraud mitigation to foster more familiarity with the pros and cons of AI in the credential review process.[viii] Until the global health community develops and adopts global certification programs with a unifying framework that standardizes the assessment and recognition of health worker competency, the risk of AI-driven credential fraud remains high.[viii]

2. Improve collaboration and coordination, inside and outside of healthcare.

Nursing credential fraud is too complex and too adaptive—especially with AI in the mix—for any one stakeholder to fight it alone. Better information-sharing and operational coordination among regulators, credential evaluators, professional associations, employers, and law enforcement is now a strategic necessity, not a nice-to-have. Combatting AI-driven credential fraud clearly requires a collective effort.

Operation Nightingale, for example, showed what is possible when coordination works: NCSBN rapidly convened updates, shared resources, offered training, hosted monthly calls for state boards, and partnered with federal agencies to align strategies and guidance in response to the Florida scandal. Stakeholders should see this as a proof of concept for ongoing, proactive coordination rather than a one-time crisis response.

Regulators can take the lead in fostering collaboration by convening regular cross-stakeholder meetings, updating fraud-mitigation playbooks and toolkits to include AI literacy and fluency and ensuring that national and international guidance flows across regulatory bodies, credential evaluators, professional associations, and employers. They can also champion and help fund empirical research on credential fraud, including AI-enabled schemes, and then disseminate those findings so others can act on them.

Stakeholders can further strengthen defenses by aligning their operational workflows: credential evaluators can tighten checks on foreign education comparability and fraud signals; regulators and boards can integrate evaluation reports with background checks, language proficiency results, and licensure exams. They can also make full use of tools like NCSBN's Falsified Identity Tracking System and Nursys® to communicate with other boards to spot and share suspicious patterns more quickly. (Nursys® is the only national database for nurse licensure, discipline, and practice privileges for RNs, LPN/VNs, and APRNs in participating boards of nursing.)

There is also a critical opportunity for nurse regulators to partner closely with AI researchers and developers. By combining their expertise, they can co-design tools, workflows, and best practices for using AI in nurse credential fraud detection and rigorously evaluate those systems.

Teams should routinely compare the performance, accuracy, and efficiency of human experts and AI-enabled systems; examine qualitative outcomes; study how bias shows up in AI tools; and track how these systems affect real-world workflows and broader sociotechnical systems. Critically, these evaluations should be publicly shared so the field can learn together and continually refine guidance for improving AI-enabled nurse credential fraud detection.

Credential evaluators and the regulators who make use of their work represent a specialized stakeholder group that plays a vital role in the ongoing fight against credential fraud. AI tools that support expert human decision-making are generally designed by AI experts working closely with those who best understand the decisions, as well as the context of decision-making, that these new systems will support. The nurse regulator community, therefore, must partner closely with AI researchers and developers to share their unique insights and collaborate to generate tools, workflows, and evidence-based guidance for using AI and related technologies in nurse credential fraud detection.

3. Partner with the technology sector to build secure, closed digital ecosystems.

The natural evolution from paper to digital credentials alone doesn't guarantee the authenticity of the "proof" presented; digital documents can still be falsified. In fact, digital document forgery surpassed physical counterfeits for the first time in 2024, with digital forgeries accounting for 57% of all document fraud.[ix] That's why credentials that are issued, validated, and shared via secure, encrypted and decentralized digital ecosystems will be critical to curtailing both traditional and AI-enabled credentials fraud.

In nursing, verifiable digital credentials turn diplomas, transcripts, and licenses into cryptographically signed records that employers can verify directly with the issuing school or board—no phone calls, PDFs, or faxed documents required. That makes it far harder for unqualified individuals to use fake or altered nursing diplomas, fabricated license numbers, or expired credentials to get hired, because any credential that isn't genuinely issued and still valid simply fails verification.

Across the globe, governments and private sector leaders have begun to accelerate their efforts to implement standards for verifiable digital credentials.

- In 2025, the World Wide Web Consortium (W3C) released its Verifiable Credentials Data Model 2.0, essentially becoming the new "web standard" way to represent digital ID cards, licenses, and other proof documents online so they can be trusted, protected against tampering, and more effectively checked by computers.
- All 27 European Union (EU) Member States are required to provide EU Digital Identity Wallets to citizens and residents by December 2026, thanks to a regulation that creates a unified "European Digital Identity Framework."
- Singapore's Singpass and India's Aadhaar are two of the world's most mature national digital ID systems. These platforms can be extended to professional credentials, giving hospitals a secure way to confirm who a nurse is without handling PDFs or screenshots.

These and other efforts signal a broader global shift toward a more secure, trustworthy infrastructure for professional credentials—one that nurse regulators and credential evaluators would be wise to help shape, not simply adopt.

Did you know?

TruMerit is developing the use of digital identities, verifiable credentials, and digital wallets in partnership with Credivera, a digital identity and workforce management solution provider. Digital wallets and digital verifiable credentials allow global healthcare professionals to securely store, manage, and share information about certifications and education, giving full ownership of these credentials to the legitimate holder and allowing them to instantly share them with employers or regulators.

TruMerit believes that building a global network of entities that rely on self-custodied digital identities and verified credentials for healthcare workers will streamline the ability for those workers to present secure credentials to regulators, employers, recruiters, and other relevant stakeholders across careers.

Currently, TruMerit issues verifiable digital credentials for all applicants who successfully pass a global certification exam (Certified Global Nurse, Certified Global Nurse – Rehab, Certified Global Health Worker – Rehab, and Certified Global Health Worker – Rehab Advanced). These high-stakes certification exams—and the requirement for ongoing revalidation of competence—provide an additional safeguard against AI-enabled credential fraud by ensuring that credentials reflect continuously demonstrated knowledge and skills, not just static claims. Future planned integration of digital credentials with our migration support services (VisaScreen® and Credentials Evaluation Services) will enable our applicants to benefit from a unified, secure digital credential portfolio.

Learn more at https://www.trumerit.org/.

Conclusion: An evolving challenge with evolving solutions

TruMerit believes the time to address AI and credential fraud head-on is now.

Recent research by the Association of Certified Fraud Examiners shows that only 7% of anti-fraud professionals say their organizations are "more than moderately prepared to detect or prevent AI-fueled fraud."[x] In a 2026 paper for The Journal of Nursing Regulation, TruMerit researchers wrote: "We recommend that regulators continue to actively take...measures such as coordinating regular meetings among stakeholder groups and updating best practice guides and toolkits on fraud mitigation to include AI literacy and relevant national and international guidance. Nursing regulators can support research and empirical studies in credential fraud and fraud detection related to AI, as they are best positioned to sway the necessary actors and coordinate impactful, research-based anti-fraud efforts."[xi]

AI is evolving at an incredible pace, so those involved in nursing credentialing should assume that today's tools, tactics, and skills will swiftly go out of date, and plan accordingly. Instead of treating an AI-enabled fraud detection system as a one-time project, regulators, credential evaluators, and technology teams should see it as a living workflow that must be tested, tuned, and retrained over time as the social, informational, technical, and regulatory landscape shifts. That means building in long-term AI-informed credential evaluation programs from the start, not bolting them on later.

Awareness, collaboration, research, and the development of evidence-based policies and guidelines are key to combatting AI-driven credential fraud. And while AI tools can greatly enhance fraud detection, human beings must remain at the center by bringing critical thinking, oversight, and integrity to every verification decision.

About TruMerit

TruMerit is a worldwide leader in healthcare workforce development. Formerly known as CGFNS International, the organization has a nearly 50-year history supporting the career mobility of nurses and other healthcare workers—and those who license and hire them—by validating their education, skills, and experience as they seek authorization to practice in the United States and other countries.

As TruMerit, this mission has been expanded to building workforce capacity that meets the needs of people in a rapidly evolving global health landscape. Through its Global Health Workforce Development Institute, the organization is advancing evidence-based research, thought leadership, and advocacy in support of healthcare workforce development solutions, including globally recognized practice standards and certifications that will enhance career pathways for healthcare workers.

Want to learn more?

Learn more about how the healthcare community can more effectively combat nursing credential fraud at https://www.trumerit.org/credentials-fraud-detection-and-prevention/.

References

[i]United States Department of Justice. (2025) National Health Care Fraud Takedown Results in 324 Defendants Charged in Connection with Over $14.6 Billion in Alleged Fraud, retrieved from https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-324-defendants-charged-connection-over-146

[ii]Herckis, L., & Tse, E. (2025) AI-enabled fraud detection, prevention, and perpetration in nursing credential evaluation: a scoping study. Journal of Nursing Regulation, 16(3): 183-194, retrieved at https://www.journalofnursingregulation.com/article/S2155-8256(25)00097-3/pdf

[iii]ZeroFox. (2025) How to Detect DeepFakes: A Guide for Security Teams, retrieved at https://www.zerofox.com/blog/how-to-detect-deepfakes/

[iv]Gartner. (2025) Mitigate rising candidate fraud through identity verification, retrieved from https://www.gartner.com/en/documents/6343879

[v]ACFE. (2024) Occupational fraud 2024: a report to the nations. Association of Certified Fraud Examiners, retrieved from: https://legacy.acfe.com/report-to-the-nations/2024/

[vi]UNESCO. (2023) Recommendation on the Ethics of Artificial Intelligence, retrieved from https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

[vii]TruMerit. (2026) 2025 Nurse Migration Report, retrieved from https://www.trumerit.org/2025-nurse-migration-report/

[viii]Herckis, L., & Tse, E. (2025)

[ix]Entrust. (2024) Deepfake Attempts Occur Every Five Minutes Amid 244% Surge in Digital Document Forgeries, retrieved at https://www.entrust.com/company/newsroom/deepfake-attacks-strike-every-five-minutes-amid-244-surge-in-digital-document-forgeries

[x]ACFE. (2026) Study: Deepfake fraud surges – and only 7% of organizations are firmly ready, retrieved at https://www.acfe.com/about-the-acfe/newsroom-for-media/press-releases/press-release-detail?s=2026-anti-fraud-technology-benchmarking-report-pr

[xi]TruMerit. (2026.) TruMerit and Credivera, retrieved from https://www.trumerit.org/verifiable-digital-credentials/credivera/