POSITION STATEMENT

Toward a Fraud-Free Environment

Background

Nurses are the largest group of professionals within the healthcare sector and are responsible for most of the direct care patients receive. Credentials evaluation and screening ensure that this care is provided safely by an appropriately skilled workforce. Already complex evaluation processes are further complicated when nurses presenting credentials are internationally educated. For them, proper verification requires expertise in educational and regulatory frameworks, as well as documentation protocols across diverse jurisdictions worldwide.

In 2023, we learned of **Operation Nightingale,** a multi-state law enforcement action that uncovered a ring of schools in Florida that sold more than 7,600 fake diplomas and transcripts to aspiring registered nurses and practical nurses. Unfortunately, with these fraudulent nursing credentials, many individuals were able to take and pass NCLEX (the U.S. national licensing examination), become licensed, and secure employment despite not having the requisite education and clinical training to do so. This incident highlighted the importance of the evaluation process in ensuring that only qualified individuals are admitted into the nursing profession and allowed to practice.

Appropriate reviews and screenings require close attention to the challenges of an evolving landscape. This effort demands consideration of the transition from paper to a more digital environment, engagement with primary source verification, and the use of a robust series of checkpoints in academic and professional data. In this way, we can and must work toward creating a fraud-free framework and conduct the credentials review responsibly and competently.

Combating fraud on multiple fronts

Moving from paper to digital records may improve efficiency and save on costs, but unsafe execution can compromise the process. For example, delivery by email is particularly prone to phishing attacks. Accordingly, just as we are advised not to transmit medical records directly via unsecured email, it is important that educational and professional credentials are delivered via secure transfer. But it doesn't end there. Primary source verification and a short chain of custody are essential to ensuring that credentials are received directly from the issuing and/or governing authorities, minimizing opportunities for tampering by another party.

However, as evidenced by **Operational Nightingale,** even a secure platform with primary source verification is still not sufficient. Combating security threats requires further diligence. Inconsistencies and irregularities can be identified through multiple layers of security, such as checkpoints against candidate biodata. The bottom line is that by weaving a framework that combats fraud on multiple fronts, we can work toward a fraud-free environment.

Basis of our solution

In response to all of this, at TruMerit™ (formerly CGNFS International) we take proactive, measurable steps to identify and combat fraud, address emerging threats, and ensure a secure, streamlined, tamper-resistant credential verification process. We do this by employing:

A secure portal—TruMerit operates a state-of-the-art Credential Transfer Portal (CTP), enabling issuing authorities to submit school and licensure records electronically and securely. We use network security technology including secure web gateways to filter traffic and enforce policy compliance. The CTP is hardened using Advanced Endpoint Protection and other web security tools.

A short chain of custody—This is at the core of our strategy for working toward a fraud-free environment. No one may access our secure portal except for those who have the authorization to issue or verify credentials.

Tightly controlled access—Only recognized educational institutions, licensing boards, or professional associations that issue credentials can share records with TruMerit via the CTP. To be a recognized CTP user, each institution must undergo a vigorous vetting process. Each school campus and department is associated with a unique account, and each must identify the authorized users for their account on the CTP. Designated portal users must also undergo a multifactorial approval process, ensuring that they have official institutional email addresses as well as the ability and authority to authenticate credentials. Institutions are also required and prompted to reconfirm their designated representatives regularly, as staff and/or their responsibilities can change.

In addition to all this, TruMerit regularly reviews each institution and every designated representative on the portal, and updates are made on a continuing basis. Portal users may not register with free email accounts such as Gmail, as the security of such accounts cannot be ensured by the schools and licensing authorities that make use of them.

Multiple layers of security—Our systems cross-reference credentials against applicant biodata and the country's educational and regulatory systems. TruMerit verifies details such as graduation dates, licensure numbers, and other relevant information. Our experts ensure that information on documents is consistent with the individual's application, and we look for any discrepancies in job titles, dates of employment, and other details. Multiple checkpoints at each stage of the review process strengthen our protocol.

Human intelligence and expertise—The varied nature and evolution of regulations and practices across international jurisdictions can be exploited by fraudsters looking to deceive regulators and employers. However, regulation at the jurisdictional level also contributes to distinct education and licensure patterns that our experts are able to identify and use in the evaluation of nursing credentials, thereby ensuring robust security. TruMerit has been maintaining and expanding proprietary archives of nursing credentials information, representing decades of expertise and significantly enhancing our ability to identify errors, inconsistencies, and irregularities of all kinds.

Toward a fraud-free environment

It is imperative that we work toward a fraud-free framework, employing digital security, primary source verification, significant redundancy and data checkpoints, and multiple layers of protection. Importantly, our tools and strategies must constantly be reevaluated and adjusted to stay ahead of fraudsters as their tactics evolve.

School and licensing officials can violate public trust, and individuals with nefarious intentions will attack even the most stringently protected systems. Inconsistencies and irregularities are identifiable through persistent and careful screening, however, especially when this work is bolstered by expertise in how educational and regulatory systems operate across the globe. Our experts in global accreditation and recognition processes, and their familiarity with the latest changes in a constantly shifting landscape, enable TruMerit to stop bad actors in their tracks.

Fraud is a dynamic international problem. We all must continue to evolve and adapt so that we can establish and maintain a fraud-free environment and so that we can protect the nurses who protect us.