



HESI exam security:

A layered defense framework for assessment integrity



Published by Elsevier | HESI Test Security Team



ELSEVIER

Advancing human progress together



Abstract

The validity of nursing licensure preparation depends on the integrity of the assessments used to predict student readiness. This white paper outlines the multi-layered security architecture that underpins HESI secure assessments, examines known threats, and presents a strategic framework for continuous improvement. The following provides an account of what HESI does to protect score validity today, and our ongoing efforts to maintain exam integrity and validity.

Why assessment security matters

Standardized nursing assessments serve an important purpose, providing an accurate, defensible indicator of a student's readiness to pass NCLEX® and safely enter clinical practice. When exam content is compromised, such as through organized sharing of answer keys, proxy test-taking, or screen capture, the score loses its meaning. Students who succeed in their programs through illicit means rather than genuine competency represent a patient-safety risk that extends far beyond academic dishonesty.

The consequences fall disproportionately on the institutions that rely on HESI results for programmatic decisions, NCLEX prediction and accreditation documentation. A compromised exam does not merely disadvantage honest students; it undermines the evidentiary basis on which nursing programs make consequential student and resource decisions.

Elsevier recognizes this responsibility and believes strongly that test security extends beyond a compliance checkbox; it is a core pillar of HESI's value to the nursing education community. This article outlines in detail how HESI approaches that responsibility.



The threat landscape

The past decade has brought increasingly sophisticated threats to standardized assessments. Three patterns in particular stand out for their impact on exam integrity and score validity.

Organized content sharing

Students increasingly use private messaging platforms, paid online services, and social media to circulate reconstructed exam questions and answer rationales from their exams. The distributed and encrypted nature of these channels makes detection difficult and takedown notices only partially effective.

Proxy and remote-assistance testing

The shift toward remote assessment created opportunities for students to use secondary devices to photograph screens, receive coached answers in real time, or permit a third party to complete the exam on their behalf via remote desktop software.

Score clustering and anomaly patterns

When large numbers of students from the same cohort score aberrantly high, most notably above 1150, it can indicate that students collaborated to improve their scores, such as by sharing advanced knowledge of the exam items.

Current HESI security architecture

HESI's security framework operates across four domains: the testing environment, access and identity controls, content protection, and pre- and post-exam online monitoring. The controls described below are active today.

Elsevier Secure Browser (ESB)

The Elsevier Secure Browser provides the primary technical control over the HESI test environment. It functions at the operating-system level, locking down browsers, and restricting what students can access or execute during an exam session. Specific capabilities include:

- Blocking virtual machines and remote desktop applications commonly used for proxy testing
- Preventing screen-sharing and screen-recording software from operating
- Disabling the clipboard to prevent copy-and-paste of question content
- Whiting out secondary monitors so adjacent displays cannot be used to display notes or receive coaching
- Disconnecting the exam session when prohibited keystrokes or application-switching is attempted
- Prohibiting navigation away from the exam environment until the session is formally exited

Live proctoring

Live proctoring is required for all HESI secure exams. Elsevier's published best practices establish a structured proctoring protocol organized around three imperatives: control the room, control the machines, and close the loop.

Key practices include:

- A recommended minimum ratio of one roving proctor per ten students to maintain active visual oversight
- A dedicated proctor to monitor the HESI real-time proctoring dashboard that surfaces behavioral alerts, including unusual patterns, as they occur
- A structured check-in process that validates student identity before exam access is granted
- When employing remote proctoring, using Elsevier-approved vendors who uphold testing policies to ensure test validity

Real-time access controls

Before an exam session begins, students must enter a virtual waiting room where a live proctor validates each student's identity and authorizes entry. Only after authorization is granted, a unique single-use access code is generated and delivered to the specific student admitted to the exam. This control prevents unauthorized exam access even if login credentials are shared.



The Swiss cheese model applied to assessment security

No single control is foolproof. A secure browser can be circumvented by a phone camera. A proctor can be distracted. An item can leak. The Swiss cheese model of system safety — originally developed in aviation and healthcare risk management — holds that layering multiple imperfect defenses ensures that the “holes” in any one layer are covered by the solidity of the others. HESI's security architecture is explicitly designed on this principle: each control listed below compensates for the limitations of the others.

Current HESI security architecture

(continued)

Content architecture: randomization and versioning

HESI reduces content exposure risk through several content controls:

- HESI exams are double-randomized where both the question order and answer-choices order are randomized independently for each test-taker
- Nearly all HESI RN and PN standardized exams have two or more parallel versions, allowing for student exam retesting and rotation of versions across cohorts
- All secure HESI exams replace a minimum of 30% of exam items three times per year, ensuring regular introduction of new content. For RN and PN Exit Exams (the final assessments students complete before taking their NCLEX), the rate increases to 40%, providing an accelerated refresh cycle so that familiarity with prior exam content provides no meaningful advantage.
- A dedicated item pipeline maintains parallel development tracks across content areas, ensuring a continuous influx of newly written, piloted, and statistically evaluated items

Student conduct agreement

Prior to every exam, each student is required to read and accept Elsevier's Student Conduct Agreement. This serves as a pre-exam gate that outlines the consequences of noncompliance and requires each test-taker to agree to participate in the exam in a responsible, secure manner.

Watermarking

HESI exam items display a visible watermark containing each student's name and unique session identifiers as a subtle overlay on every screen. The watermark serves a dual purpose: as a deterrent, the visible identifier signals to students that any photo taken is traceable back to them; and as an investigative tool, should unauthorized content surface, the embedded identifiers allow Elsevier to trace the source and take appropriate action.



Content fraud investigations and web patrol

The HESI Test Security Team monitors the internet for unauthorized postings of, or claims about, HESI exam content. If and when content is identified, the team:

- Initiates a formal investigation
- Issues takedown notices to hosting platforms
- Works with legal counsel and third-party vendors to pursue removal of unauthorized content
- Adjusts exam content when the scope of exposure warrants action

Computerized Adaptive Testing (CAT)

HESI's CAT is available as an end-of-program assessment. The exam adapts in real time to each student's performance, drawing different items from the calibrated item bank as the assessment progresses. The unique item path each student follows limits answer-sharing and helps ensure scores reflect individual performance.

Psychometrically sound item development

All HESI exam items are developed and maintained using advanced psychometric methods. Item and test statistics are used systematically to evaluate the quality, difficulty and discrimination properties of each item. Ongoing content review ensures that the exam blueprint remains aligned with current nursing competency frameworks and that underperforming or exposed items are flagged for revision or retirement.

Conclusion

Protecting the integrity of an exam is ongoing work. No single safeguard keeps an assessment secure on its own. It requires steady, coordinated attention as the testing and technology landscape continues to change. The threat environment will also continue to evolve, and so will HESI's response to it. The architecture described in this article represents a layered approach to score validity, built on the understanding that no single control is sufficient on its own.

Elsevier's Test Security Team remains committed to transparency with institutional partners. Our goal is to give nursing faculty and administrators the confidence of knowing the HESI scores they use to make consequential decisions reflect genuine competency and readiness for NCLEX.

For questions about HESI exam security practices, to report a suspected compromise or to learn more about institutional best practices, contact your Elsevier Sales Representative.

