HIPAA/HITECH Risk Assessment Professional Report

Prepared for:

Nesso Labs

125 S King Street, Suite 2A

Jackson, WY 83001-1045

Audit Period: December 15, 2025 - February 15, 2026

Risk Assessment Performed and Professional Report prepared by:

VANREIN COMPLIANCE

VanRein Compliance has successfully concluded a comprehensive HIPAA/HITECH Security Risk Assessment for Nesso Labs . Our thorough assessment was reflective of the HIPAA Security Rule's stipulations concerning security measures, incident management, risk mitigation strategies, and employee protocols.

Nesso Labs is the EHR that understands therapists—designed to guide solo therapists and small group practices through decisions, whether simple or complex, with clarity, conviction, and care.. They were assessed for complete compliance of the HIPAA and HITECH regulation including documented Privacy, Security, training policies, and Business Associate agreements.

VanRein Compliance has evaluated potential risks and weaknesses that could affect the protection of Nesso Labs ' patient health information (PHI), focusing on its confidentiality, integrity, and availability within Nesso Labs systems. As mandated by the HIPAA Security Rule, it is imperative for healthcare entities, insurers, and their Business Associates to perform such risk assessments to identify and address potential vulnerabilities in their handling of Electronic Protected Health Information (ePHI). By proactively identifying and mitigating risks, these organizations can strengthen their defenses against data breaches and ensure the ongoing protection of sensitive patient information.

By partnering with VanRein Compliance to conduct a HIPAA/HITECH Security Risk Assessment, Nesso Labs has taken a proactive step towards ensuring the protection of their patients' sensitive health information. The assessment has provided Nesso Labs with valuable insights into their security posture and has equipped them with the knowledge and tools they need to maintain compliance with HIPAA regulations and safeguard ePHI against unauthorized access, use, or disclosure.

Thank you!

CoFounder | Compliance Guide | VanRein Compliance

VanRein Compliance's Professional Report

We have examined Nesso Labs assertion of the health information security program. Nesso Labs is the EHR that understands therapists—designed to guide solo therapists and small group practices through decisions, whether simple or complex, with clarity, conviction, and care. Nesso Labs accurately presented that the health information security program which includes essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009, and is presented in accordance with the criteria set forth in Nesso Labs 's assertion. Nesso Labs ' management is responsible for the assertion.

Our examination was conducted in accordance with attestation standards established by the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"). As part of the assessment, key stakeholders and IT personnel were interviewed to gain insights into operational and security practices. All applicable controls were examined to ensure alignment with industry standards and regulatory requirements. Additionally, live evidence, including screenshots and documented artifacts, was reviewed and securely uploaded to the VanRein Document Portal.

VanRein Compliance, in our opinion, and in all material respects, based on the criteria reviewed during the risk assessment asserts that the health information security program governing the handling of PHI and ePHI by Nesso Labs includes essential elements of HIPAA and HiTECH.

This report and the results thereof are intended solely for the information and use of Nesso Labs prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- Scope of Services Provided by the Organization
- System Interactions and Integration
- Internal Controls and Their Constraints
- User Responsibilities in Compliance
- Overview of the HIPAA Security Program
- Potential Risks and Mitigation Strategies

Serving You,

CoFounder | Compliance Guide | VanRein Compliance

Nesso Labs Management Report

VanRein Compliance has prepared the description of Nesso Labs's health information security program as of the audit period of December 15, 2025 - February 15, 2026. To the best of our knowledge and belief, we confirm that:

A. Management's description accurately represents the health information security program for Nesso Labs. The criteria used in making this assertion were:

- The description accurately reflects how the health information security program was designed and implemented to govern security policies and practices. It outlines the specified controls within the security program, ensuring alignment with the program's objectives.
- No relevant information about Nesso Labs's health information security program has been omitted or misrepresented. However, the description may not include every detail that an individual user entity may consider significant in its specific environment.

B. Nesso Labs's health information security program incorporates key elements of HIPAA and HITECH. The criteria used in making this assertion were:

- Management identified and established the applicable controls (the "controls") included in the health information security program.
- The documented controls align with the standards and implementation guidance outlined in the HIPAA Security Rule, covering the following areas:
    - Administrative Safeguards
    - Physical Safeguards
    - Technical Safeguards
    - Organizational Requirements
    - Policies, Procedures, and Documentation Requirements
    - Breach Notification

Oleg Bagatskyy

_____ | Oleg Bagatskyy | Compliance Officer | Nesso Labs

Signature

Health Information Security Program

Nesso Labs has established a health information security management program to ensure compliance with information security requirements and effectively provides a clinical documentation tool and practice management solution for therapists. This program integrates key elements of HIPAA and HITECH to safeguard protected health information (PHI).

The following description provides a summary of the safeguards Nesso Labs has implemented to align with the applicable provisions of the HIPAA Final Security Rule and the breach notification requirements under HITECH.

Administrative Safeguards

- **Security Management Process.** HIPAA Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.
- **Assigned Security Responsibility.** HIPAA Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
- **Workforce Security.** HIPAA Standard: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
- **Information Access Management.** HIPAA Standard: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
- **Security Awareness and Training.** HIPAA Standard: Implement a security awareness and training program for all members of its workforce (including management).
- **Security Incident Procedures.** HIPAA Standard: Implement policies and procedures to address security incidents.
- **Contingency Plan.** HIPAA Standard: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
- **Evaluation.** HIPAA Standard: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
- **Business Associate Contracts and Other Arrangements.** HIPAA Standard: A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information.

Physical Safeguards

- **Facility Access Controls.** HIPAA Standard: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- **Workstation Use.** HIPAA Standard: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
- **Workstation Security.** HIPAA Standard: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
- **Device and Media Controls.** HIPAA Standard: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Technical Safeguards

- **Access Control.** HIPAA Standard: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- **Audit Controls.** HIPAA Standard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
- **Integrity.** HIPAA Standard: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
- **Person or Entity Authentication.** HIPAA Standard: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
- **Transmission Security.** HIPAA Standard: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Organizational Requirements

- **Business Associate Contracts or Other Arrangements.** HIPAA Standard: (i) The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in §164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—(A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.

Policies and Procedures and Documentation Requirements

- **Policies and Procedures.** HIPAA Standard: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
- **Documentation.** HIPAA Standard: (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

Breach Notification

The HIPAA Breach Notification Rule, 45 CFR §164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Periodic Risk Assessments and Risk Management

Nesso Labs has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by Nesso Labs to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires Nesso Labs to identify risk based on management's internal knowledge of its operations.

The purpose of a risk assessment is to identify conditions where ePHI could be disclosed without proper authorization, improperly modified, or made unavailable when needed. This information is then used to make risk management decisions on whether the HIPAA-required implementation specifications are sufficient or what additional addressable implementation specifications are needed to reduce risk to an acceptable level.

Standard 164.308(a)(1)(i), Security Management Process, requires covered entities to:
Implement policies and procedures to prevent, detect, contain, and correct security violations. The Security Management Process standard includes four required implementation specifications. Two of these specifications deal directly with risk analysis and risk management.

1. **Risk Analysis.** HIPAA Standard § 164.308(a)(1)(ii)(A): Perform a precise and comprehensive evaluation of possible threats and weaknesses concerning the confidentiality, integrity, and accessibility of ePHI maintained by the organization or its partners.
2. **Risk Management.** HIPAA Standard § 164.308(a)(1)(ii)(B): Establish and execute security protocols adequate to diminish identified hazards and vulnerabilities to a level that is both logical and suitable for achieving compliance with § 164.306(a).

nesso

Risk Assessment Performed and Professional Report Prepared by:

VANREIN COMPLIANCE

The information and results listed in this Risk Report were crafted from information provided to VanRein Compliance by the client. Recommendations by VanRein Compliance is not meant to be legal recommendations but industry standard and HIPAA/HITECH Regulations