



To: Doug Ridyard, MD; Founder, Eleanote

Re: System Level HIPAA Security and Risk Analysis Assessment for Eleanote Desktop software Application

Date: May 14, 2026

This document serves as a formal letter of attestation for the recent system level HIPAA Security Gap and Risk Analysis review undertaken for Eleanote by RMHG, a qualified third party, with a focus on Eleanote's desktop software application implementation hosted at Amazon Web Services. As part of this engagement, RMHG analyzed a subset of HIPAA Security Rule safeguards applicable to Eleanote's desktop software application architecture, workflow, and functionality, in addition to assessing the risk of threats to electronic protected health information ("ePHI") handled by the desktop software application. RMHG performed this analysis between the dates of April 25, 2026, and May 14, 2026.

The following frameworks were utilized for the assessment:

- National Institute for Standards in Technology (NIST) Special Publication (SP) 800-66 Rev 2: "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide"
- NIST SP 800-30 Rev 1: Guide for Conducting Risk Assessments
- US Department of Health and Human Services (HHS) and Center for Medicare and Medicaid Services HIPAA "Security Series"

Based on the evidence collected from this system level HIPAA Security Rule compliance review and risk analysis, RMHG has concluded in its professional opinion that Eleanote has designed and implemented security controls that satisfy all applicable system level HIPAA Security Rule safeguard requirements, in addition to reducing all critical and high threat risks to medium or low threat risks.

RMHG believes that the statements made in this letter provide an accurate assessment of Eleanote's desktop software application information security posture as it relates to system level HIPAA Security Rule safeguard requirements and risk of threats to ePHI. As the Eleanote desktop software application, information technology environment, and business processes may change over time, the information security posture may change as well. Therefore, the conclusion reached from this analysis represents a point-in-time review and attestation. RMHG thanks Eleanote for this opportunity to assist with evaluating the desktop software application system level HIPAA Security Rule compliance posture.

Sincerely,

A handwritten signature in black ink, appearing to read "Andrew Labbo".

Andrew Labbo
MBA, CISSP, ITIL
Principal and Owner
RMHG LLC, www.rmhguru.com