SAMPLE REPORT

48-Hour Shadow Audit

Executive Findings & Evidence Summary

Engagement Overview

Client	Redacted Healthcare Firm (HIPAA-covered entity)
Population	1,000 active users across clinical, finance & executive teams
Audit Window	March 15, 2026 00:00 ET – March 17, 2026 00:00 ET (48 hours)
Mode	Shadow Audit — passive detection, no end-user notifications, no auto-ejection
Platforms Monitored	Microsoft Teams, Zoom, Google Meet
Report ID	NTG-SA-2026-0317-RHF
Prepared By	NotetakerGuard Compliance Operations

1. Executive Summary

Over a continuous 48-hour observation window, NotetakerGuard ran in Shadow Mode across the client's Microsoft Teams, Zoom, and Google Meet tenants. The platform passively classified every meeting participant against its bot-detection signal set without generating notifications, removals, or user-visible activity.

The audit confirmed a material, previously-undetected exposure of confidential conversation content to third-party AI notetakers and recording bots that were not on the client's approved vendor list.

Headline Findings

14	8	3	0
Unauthorized AI bots detected	Attempted joins to executive-level meetings	Successfully captured PII before manual ejection	Flagged by existing DLP / EDR / CASB stack

Every detection in this report was independently corroborated by at least two signals (name pattern, join behavior, network fingerprint, or vendor API metadata).

2. High-Risk Meetings Targeted

The following executive-tier sessions were targeted by unauthorized bots during the audit window. Names have been redacted; meeting IDs and full audit trails are available in the encrypted evidence bundle.

Meeting	Date & Time	Bots Detected
Q1 Board Meeting	March 15, 2026 — 2:00 PM ET	**2 unauthorized bots**
M&A Strategy Session	March 16, 2026 — 10:30 AM ET	**3 unauthorized bots**
Client Onboarding Call	March 17, 2026 — 9:00 AM ET	**1 unauthorized bot**

Representative Incident — Q1 Board Meeting

- 14:00:32 ET — Meeting started. 11 human participants joined.
- 14:03:11 ET — Bot "Otter.ai Notetaker" joined via guest link. Classified as Notetaker (confidence 0.94).
- 14:07:48 ET — Bot "Fireflies.ai Fred" joined under organizer's calendar invite. Classified as Notetaker (confidence 0.91).
- Neither bot was registered to the client's approved-vendor list. Both remained until the host adjourned the meeting at 15:02 ET.
- Estimated transcript exposure: ~62 minutes of board-level financial discussion.

3. Control Gap Analysis

The client's existing stack did not surface any of the 14 detections during the audit window:

- DLP — Content-only inspection; bots produced no policy-matching artifacts in scanned channels.
- EDR — Endpoint-resident; cloud-to-cloud bot joins never touched managed devices.
- CASB — Detected sanctioned SaaS sessions but had no signature for unsanctioned meeting bots.
- Calendar governance — Bots joined via forwarded invites and guest links that bypassed organizer review.

4. Risk & Regulatory Impact

Given the client's HIPAA-covered status and the content discussed in the targeted meetings, the captured PII constitutes a reportable exposure under 45 CFR §164.402 absent a documented Business Associate Agreement with each detected vendor. Recommended response actions:

- Immediately review BAA coverage for Otter.ai, Fireflies.ai, and the two additional vendors listed in Appendix A.
- Engage privacy counsel on §164.402 risk-of-compromise assessment for the 3 PII-capture events.
- Notify affected executives and clients per the client's incident-response runbook.

5. Recommendation

NotetakerGuard recommends transitioning from Shadow Mode to Enforced Mode for all three platforms. In Enforced Mode the same detections complete end-to-end ejection in under 1.5 seconds, preventing any transcript capture.

- Deploy Enforced Mode for executive and clinical meeting rooms within 5 business days.
- Onboard the approved-vendor allow-list for Otter, Fireflies, Read.ai, and Fathom (if retained).
- Wire SIEM forwarding for every ejection event into the client's Splunk index.
- Schedule a 30-day re-audit to validate residual exposure has reached zero.

6. Evidence & Chain of Custody

A signed, encrypted evidence bundle accompanies this report and contains:

- Per-meeting participant rosters with detection factors, confidence scores, and SHA-256 hashes.
- Network metadata (provider ASN, JA3 fingerprint, user-agent) for every flagged bot.
- SIEM-ready CEF export of all 14 detections.
- Tamper-evident audit log signed with NotetakerGuard's compliance key (fingerprint on file).

— End of sample report —