CASE-NOVA

Security protocols

Presented by 9 to 5 Office

November 8, 2026

This one-page summary describes controls Case-Nova uses to protect practice and examinee data, as implemented in the product and its Google Cloud hosting.

ENCRYPTION

- Examinee names, dates of birth, notes, contact details, appointment text, invoices, and document tokens are encrypted in the application with dual-layer AES-256-GCM before they are stored.
- Uploaded records and practice backups are encrypted with the same method before they are written to disk or Cloud Storage.
- The encryption key is kept in Google Secret Manager in production, not in the application image.

SIGN-IN AND SESSIONS

- Passwords are stored with bcrypt (cost 12). They must be at least 10 characters with a number and a symbol, expire every 6 months, and cannot be reused.
- Temporary passwords must be changed at first sign-in.
- Sign-in uses an email code and/or an authenticator (TOTP). A trusted browser can skip the code for 7 days.
- A new browser emails the account holder the IP address so they can approve it or report it.
- Sessions use HttpOnly cookies, signed with HMAC. Production cookies are marked Secure. Idle sign-out is 30 minutes; the session ends after 8 hours.

WHO CAN SEE WHAT

- Each practice is its own workspace. Staff only see that practice’s records.
- Evaluator and Admin roles limit notes, record review, billing, and time tracking.
- Assigned evaluators see only the examinees given to them unless they are the primary evaluator or an admin for that practice.
- A practice can be suspended. Records stay stored; sign-in is blocked until access is restored.
- The cross-practice access log is limited to designated 9 to 5 Office accounts.

AUDIT, DOCUMENTS, AND REPORTS

- Sign-ins and opens of examinees, records, invoices, and exports are written to an access log. Payload details (including IP) are encrypted.
- Intake and other outbound documents are sent as a private HTTPS link, not as an emailed PDF attachment. Signing records include name, email, time, and technical details.
- Completed signed PDFs can be sealed. Report PDFs can require a password that Case-Nova does not keep.
- Uploads are capped at 50 MB per file. Zip files are not allowed.

HOSTING AND THE BROWSER

- Production runs on Google Cloud Run with Cloud SQL (PostgreSQL) and a private Cloud Storage bucket.
- HTTPS is required in production, with HSTS, a content security policy, frame restrictions, and related browser security headers.
- Google Drive and Google Meet use OAuth on a registered redirect URI. Tokens are stored encrypted per connection.

This describes product and hosting controls. Case-Nova is practice software. It is not a certified EHR and is not a HIPAA certification. Practices remain responsible for their own policies, staff access, and the Google accounts they connect.