Prior Auth Denial Prevention Checklist

Stop the denial before you submit. Organized by the reasons claims actually get denied. | ClinicOps

Most denials are preventable. Half of providers name missing or inaccurate data as the top driver (Experian, 2025), which means the fix happens at the desk, before submission, not in an appeal afterward. Run this before every request.

Denial reason	Prevent it by checking, before you submit
■ Missing / inaccurate data (the #1 cause)	Patient, plan, and group numbers match the card exactly. Demographics and date of birth verified. No typos.
■ No authorization on file	This service needs auth for THIS plan. Auth obtained before the service. Auth number and expiration recorded.
■ Eligibility / coverage	Coverage is active on the date of service and the service is covered. Verified before the visit, not after.
■ Coding mismatch	CPT or HCPCS and ICD-10 support each other. You used the codes this payer requires.
■ Insufficient documentation	You attached what the payer's reviewer wants to see for medical necessity, not just what you assume proves it.
■ Timely filing / expired auth	Submitted inside the filing window. Auth will not expire before the date of service.

THEN: LOG EVERY DENIAL AND FIX YOUR TOP PATTERN

Prevention catches most. For the rest, log every denial with its reason, then count. Whatever reason shows up most is your practice's specific leak. Fix that one root cause and you remove a whole category of future denials, not one claim at a time.

Track it on your denial log: reason, owner, appeal deadline, and dollar amount. Work each one to paid, and review the reason counts monthly.

THE ONE RULE: Chart numbers only. No patient name, date of birth, or diagnosis in any log or board. The board holds the workflow; your EHR holds the patient.