Privacy and Security

What stays local, what may leave the workstation, and the realistic limits of local software protection.

Local case-package processing

Production Package Doctor processes selected production-package contents on the operator's Windows computer. The operator selects both the source package folder and the report destination folder. Reports are written only to the operator-selected report folder.

No case-data upload

The desktop application does not upload DAT, OPT, image, text, native, report, or derived case content. Limited authorization, lease-refresh, device-lifecycle, and opaque Pilot-accounting data may be exchanged with the owner-controlled authorization service.

Read-only source behavior

The application reads the selected source package and writes reports to a separate operator-selected location; it does not repair or rewrite the source package. Source files are opened read-only during the audit.

Limited authorization traffic

When the product is activated for the Pilot, a small amount of opaque metadata is exchanged for license activation, lease refresh, and device lifecycle. This traffic does not include case data, reports, or source package contents.

Report-location control

The operator chooses where reports are saved. The application does not send reports to a remote server, cloud storage, or shared workspace unless the operator explicitly copies them there.

Realistic limits of local software protection

The protected local build is intended to deter casual copying and analysis. No local software can guarantee that determined analysis is impossible. Physical access, administrative rights, and sufficient time can defeat any local protection mechanism.