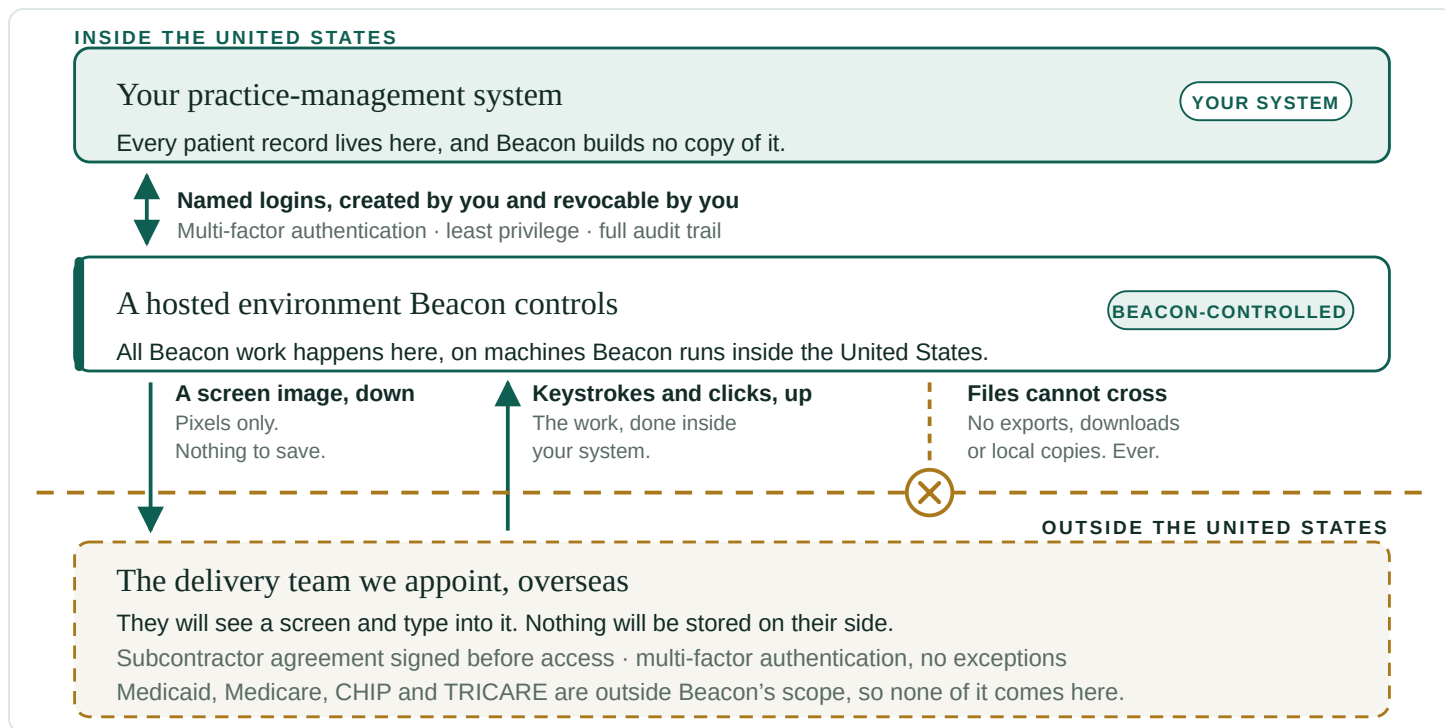


SECURITY OVERVIEW

Where your patient data goes. Two places, both named in your agreement.

Your patient records stay in your practice-management system. The insurance data we work on is handled inside our own United States-hosted environment, under the business associate agreement you sign, and nowhere else.



OUR COMMITMENT ON COMPLIANCE, STATED PLAINLY

Business associate agreement	Signed before any access
Written HIPAA security policies	In force before we hold your data
Annual security risk analysis	Completed before we hold your data
Named security officer	Appointed, named in your agreement
Cyber and errors-and-omissions cover	Bound before your start date
Massachusetts security program	In force before we hold your data
Subcontractor agreement	Signed before any access

WHAT WE WILL SEND YOU BEFORE YOU COMMIT

- ✓ Our business associate agreement, in full
- ✓ The client agreement and Schedule C, where the floors sit
- ✓ The access model, and the named people once your team is assigned
- ✓ Our subcontractor terms, cross-border clauses included

Every item in that table is a commitment we make before your start date, not work already done for someone else. We are new, and we would rather say so.

De-identified data, said out loud. Beacon strips identity from the billing data it works with and will pool it to spot payer patterns. We maintain and use it only in de-identified form, we do not attempt to re-identify it, and we bind anyone we share it with to the same. Your practice is never named externally without your written permission.