



AI-READINESS DATA ASSESSMENT · SECURITY & DATA HANDLING

Your data stays **where your controls are.**

How an assessment handles your data, from first access to deletion.

DEFAULT LOCATION

Inside your environment

ACCESS

Read-only, approved by you

AGREEMENTS

Your NDA and security review

INSURANCE

E&O and cyber liability

01 Where the work happens

- By default, profiling runs inside your environment, under your access controls, on infrastructure you provide.
- We ask for read-only access to the in-scope systems or to extracts from them. We never write to production systems.
- We profile samples. Full production loads aren't required.

WHY So your data stays where your controls already apply.

02 If data has to move

- Only if you choose. Where profiling in place isn't practical, extracts move over a secure transfer method you approve.
- Transferred extracts are kept only for the engagement and deleted at the end of it.

WHY So any copy that exists has a known route, a known holder and an end date.

03 Sensitive data: PII and PHI

- Profiling measures fields and tables: completeness, validity, duplicates and how records link across systems.
- Nobody reviews individual claims, members or patient cases.
- Sensitive fields can be masked before profiling, or profiled inside your environment so they never leave it.

WHY So the assessment answers questions about the data without exposing the people in it.

04 Who has access

- Only the people on the engagement who profile the data: the principal and the analyst, named to you before access is granted.
- Our project manager coordinates scheduling and logistics and doesn't need data access.

WHY So you know exactly whose accounts to provision, and whose to revoke.

05 Agreements before access

- We sign your NDA and complete your vendor security review before any data access, and plan the start date around it.
- We carry professional liability (E&O) and cyber liability insurance; certificates are available on request.

WHY So security and legal sign off first, and the six weeks start cleanly once access is in place.

06 At the end

- Your team revokes our access at the close of the engagement.
- Any transferred data is deleted, and we confirm the deletion in writing.
- The deliverables are yours: report card, gap list, roadmap and read-out.

WHY So nothing of yours outlives the engagement on our side.

Questions this sheet doesn't answer?

Send us your security questionnaire; we complete it before any data access.

Email · info@emisile.net

Online · emisile.net/security