# I.M.P.A.C.T. — Sample MCIC Starter Kit

Illustrative example: Fictional privately owned outpatient physician practice in Texas

**Educational example only.** These are real regulatory references with illustrative applicability and evidence questions. They have not been reconciled to the current Healthcare_TX governed obligation IDs and are not an operational MCIC, compliance determination, or exhaustive assessment.

### 1. Risk analysis — 45 CFR §164.308(a)(1)(ii)(A)

**MCIC question:** For a covered entity or business associate, has an accurate and thorough analysis of potential risks and vulnerabilities to electronic protected health information been completed?

**Illustrative evidence:** Documented risk analysis, assessment date, scope, identified risks and vulnerabilities.

### 2. Notice of Privacy Practices — 45 CFR §164.520

**MCIC question:** Where notice requirements apply, does the practice maintain a current notice and provide it as required?

**Illustrative evidence:** Current notice, revision/effective date, relevant distribution or acknowledgment records.

### 3. Workforce security — 45 CFR §164.308(a)(3)

**MCIC question:** What policies and procedures govern authorization and access to electronic protected health information by workforce members?

**Illustrative evidence:** Access-management policies, authorization records, supporting access documentation.

### 4. Contingency plan — 45 CFR §164.308(a)(7)

**MCIC question:** What contingency plans protect information systems containing electronic protected health information?

**Illustrative evidence:** Data backup, disaster recovery, emergency-mode operation plans and related records.

## How this works

A governed obligation establishes what must be assessed. Applicability questions establish whether it applies to the organization. Evidence requests identify the records needed to assess the requirement. I.M.P.A.C.T. evaluates the supplied information within the agreed scope and produces PASS / RISK / FAIL findings and a separate assessment certificate.

Do not submit protected health information, patient records, or confidential evidence through the public inquiry form. Actual artifact submission requires an approved secure process following engagement and authorization.