SUMATOSOFT

Healthcare Software Vendor Evaluation Checklist

1. Certifications

Questions:

- Do you have any of the following certifications: ISO 13485, ISO 27001, SOC 2 Type II?
- Is your team trained in HIPAA compliance?
- Can you share audit reports or certification documentation?

Desirable Outcomes:

- Vendor holds valid ISO 27001 and/or SOC 2 Type II certifications.
- Has experience or certification with ISO 13485 if working on device-related software.
- Staff is trained on HIPAA compliance with documentation.
- Can show proof (certificates, internal policies, or audit summaries).

2. Experience with Clinicians or Medical Workflows

Questions:

- Have you designed solutions validated by clinicians or medical staff?
- Can you share how your UX design addresses real-world clinical workflows?
- Do you include clinicians in user testing or advisory roles?

Desirable Outcomes:

- Direct collaboration with clinicians or hospitals.
- UX research includes interviews or feedback loops with healthcare professionals.
- Shows awareness of cognitive load, workflow bottlenecks, and medical terminologies.

3. Health-specific Technology Stack

Questions:

- Are you experienced with SMART on FHIR, HL7, and X12 integrations?
- What backend and database technologies do you use for healthcare projects?
- Have you integrated with major EHRs (Epic, Cerner) or governmental portals?

Desirable Outcomes:

- Familiarity with FHIR, HL7 v2/v3, SMART on FHIR, and X12.
- Proven use of secure, scalable technologies (e.g., PostgreSQL, Kafka, MongoDB).
- Successful EHR integration or access to App Orchard / Cerner Code.
- Experience with health data exchange platforms or national HIEs.

4. Standards for Health Data Exchange

Questions:

- Which interoperability standards have you implemented?
- How do you manage clinical vocabularies (LOINC, SNOMED CT, ICD-10)?
- Do you support image formats and exchange (DICOM)?

Desirable Outcomes:

- Support for FHIR and HL7 with real implementation experience.
- Proper use of clinical coding systems (LOINC, SNOMED CT, ICD-10).
- Use of DICOM in relevant contexts (e.g., radiology apps).
- Strong understanding of regional or country-specific data standards.

5. Security Risk Management

Questions:

- Can you describe a past security risk you encountered and how you resolved it?
- What practices do you follow to ensure data is secure in transit and at rest?
- What security testing and monitoring processes do you have in place?

Desirable Outcomes:

- Transparent description of security incidents and mitigation steps.
- Encryption at rest and in transit, use of secure authentication and RBAC.
- Regular vulnerability assessments or penetration testing.
- Monitoring tools (e.g., SIEM) and alerting in place.

This checklist can be used during interviews, RFPs, or vendor assessments to help ensure you choose a partner with proven experience, regulatory knowledge, and reliable technology foundations.

SUMATOSOFT

Thank you for your time!

Any questions? Drop us a line!

Headquarters

One Boston Place, Suite 2602
Boston, MA 02108, United States

Other ways to get in touch

info@sumatosoft.com
sumatosoft.com