

# 2026 Healthcare Software Vendor Evaluation Checklist

Score each vendor on a 1–5 scale per criterion. Total score out of 175.

How to Use This: Run every vendor on your shortlist through all 7 criteria before your final decision meeting. Use the diagnostic questions verbatim – the specificity of answers matters more than the answers themselves. A vendor scoring below 105 (60%) should not advance to contract negotiation regardless of price.

## CRITERION 1 - Portfolio Matched to Your Regulatory Complexity (Weight: High ×5)

| Evaluation Point                                                                  | Score 1-5 | Notes |
|-----------------------------------------------------------------------------------|-----------|-------|
| Has built projects in your specific product category, not just general healthcare |           |       |
| Can name compliance frameworks applied to comparable projects                     |           |       |
| Willing to describe what went wrong on a prior project and how they resolved it   |           |       |
| Provides at least two references from projects with similar regulatory complexity |           |       |
| Portfolio includes production systems, not just prototypes or MVPs                |           |       |

Ask this: Walk me through a project with similar regulatory requirements to ours. What compliance framework was applied, which systems did it integrate with, and what went wrong? Score:  / 25

## CRITERION 2 - Compliance Designed In, Not Checked at the End (Weight: High ×5)

| Evaluation Point                                                              | Score 1-5 | Notes |
|-------------------------------------------------------------------------------|-----------|-------|
| Describes PHI architecture as a design input, not a post-development review   |           |       |
| Has a defined process for handling PHI in development and QA environment      |           |       |
| Manages BAA obligations across their full subcontractor chain                 |           |       |
| Has supported a client through a third-party HIPAA security audit or pen test |           |       |
| Can describe audit trails, role-based access, and encryption key management   |           |       |

Ask this: How do you handle patient data in your development and QA environments, and how do you manage BAA obligations with your subcontractors? Score:  / 25

CRITERION 3 - Production EHR Integration Experience  
(Weight: High ×5)

| Evaluation Point                                                                  | Score 1-5 | Notes |
|-----------------------------------------------------------------------------------|-----------|-------|
| Has active production integrations with EHRs relevant to your project             |           |       |
| Can describe real production problems that didn't appear in sandbox testing       |           |       |
| Understands operational differences between EHR-specific API implementations      |           |       |
| Has applications registered in EHR developer programs with production credentials |           |       |
| Has a defined process for handling EHR API version changes in live systems        |           |       |

Ask this: Which EHR platforms do you have active production integrations with today? Tell me about a production problem you encountered that wasn't documented. Score: \_\_ / 25

CRITERION 4 - Regulatory Knowledge Matched to Your Product Category (Weight: High ×5)

| Evaluation Point                                                               | Score 1-5 | Notes |
|--------------------------------------------------------------------------------|-----------|-------|
| Knows which specific regulatory frameworks apply to your product type          |           |       |
| Has navigated those frameworks on previous projects — not just read about them |           |       |
| Can provide references from projects under the same regulatory framework       |           |       |
| Proactively raises regulatory considerations relevant to your product scope    |           |       |

Ask this: What regulatory frameworks have you worked under on healthcare projects, and can you provide a reference from a project that used the same framework as ours? Score: \_\_ / 25

CRITERION 5 - The Delivery Team: Who They Are, Not Who Pitched You  
(Weight: Medium ×3)

| Evaluation Point                                                              | Score 1-5 | Notes |
|-------------------------------------------------------------------------------|-----------|-------|
| Name the specific people who will work on your project before you sign        |           |       |
| Individual engineers have direct healthcare software experience               |           |       |
| A named technical lead owns all architectural decisions, not just a PM        |           |       |
| Team has demonstrated stability, not assembled project-by-project             |           |       |
| Willing to arrange a meeting with the delivery team before contract execution |           |       |

Ask this: Who specifically - names and backgrounds will own the technical decisions on my project? Can I meet them before we sign? Score: \_\_\_\_ / 25

CRITERION 6 - Long-Term Client Relationships You Can Verify  
(Weight: High ×5)

| Evaluation Point                                                                    | Score 1-5 | Notes |
|-------------------------------------------------------------------------------------|-----------|-------|
| Provides references from clients with 2+ year engagements                           |           |       |
| References can speak to how the vendor performed during a difficult period          |           |       |
| Client retention in healthcare engagements is demonstrably high                     |           |       |
| References include projects with comparable regulatory and integration complexity   |           |       |
| Reference clients are willing to discuss commercial as well as technical experience |           |       |

Ask this: Can you connect me with a client who has been with you for at least 2 years and whose project required the same level of regulatory complexity as mine? I want to ask them about the hardest period in the engagement. Score: \_\_\_\_ / 25

CRITERION 7 - A Commercial Model Built for Healthcare Complexity  
(Weight: Medium ×3)

| Evaluation Point                                                                       | Score 1-5 | Notes |
|----------------------------------------------------------------------------------------|-----------|-------|
| Proposal accounts for regulatory complexity, not just features and timelines           |           |       |
| Has a clear process for scope changes driven by compliance or EHR updates              |           |       |
| Post-launch maintenance is priced and scoped explicitly, not described as availability |           |       |
| SLA commitments for production issues are defined in writing                           |           |       |
| Engagement structure supports long-term regulatory update management                   |           |       |

Ask this: How have you handled situations where a regulatory requirement changed the scope mid-development? How was that reflected commercially? Score: \_\_ / 25

Scoring Your Platform

| Criterion                                     | Max | Vendor A | Vendor B | Vendor C |
|-----------------------------------------------|-----|----------|----------|----------|
| 1. Portfolio matched to regulatory complexity | 25  |          |          |          |
| 2. Compliance designed in                     | 25  |          |          |          |
| 3. Production EHR                             | 25  |          |          |          |
| 4. Regulatory knowledge for your category     | 25  |          |          |          |
| 5. Delivery team                              | 25  |          |          |          |
| 6. Long-term client                           | 25  |          |          |          |
| 7. Commercial model                           | 25  |          |          |          |
| Total                                         | 175 |          |          |          |

Below 105 → Do not advance to contract negotiation 130+ → Strong shortlist candidate 150+ → High confidence selection

# Red Flag Checklist

Each red flag reduces confidence regardless of the total score

- ☐ Compliance is described as a final review phase
- ☐ Healthcare claims with no specific project names, frameworks, or integrations
- ☐ The delivery team is different from the team presented in the pitch
- ☐ Post-launch support is described as availability, not a defined model
- ☐ References don't match the regulatory complexity of your project
- ☐ Proposal doesn't address PHI architecture, audit trails, or BAA structure
- ☐ Fixed-price bid with no contingency for regulatory-driven scope changes
- ☐ No evidence of production EHR integrations, only sandbox experience cited

Next step: If you want a direct technical assessment of your project and which vendor types are actually qualified for it, **Schedule your discovery session with NonStop io Technologies.**