LegalSifter

ANY HEALTHCARE VENDOR AGREEMENT · HIPAA & REGULATORY REVIEW

The Healthcare Contract Checklist

What to require, and what to reject in any vendor agreement — read from the side that answers to HIPAA, CMS, and the OIG.

Protected health information

- ☐ **Business associate agreement** ALL / PHI **Require:** a signed BAA governs any vendor that creates, receives, maintains, or transmits PHI, incorporated into the agreement.
  Watch for: PHI access with no BAA, a BAA that caps the vendor's HIPAA obligations, or a "we are not a business associate" recital the facts don't support.
- ☐ **Data security controls** SaaS / SERVICES **Require:** encryption in transit and at rest, multifactor authentication, malware controls, and a written vendor security plan.
  Watch for: "commercially reasonable" security with no specifics, offshore data handling you never approved, or a refusal to commit to encryption or testing.
- ☐ **Breach and incident notification** SaaS / ALL **Require:** prompt written notice of any incident affecting PHI, within a fixed period, the vendor bearing the breach-response costs it causes.
  Watch for: notice only "as required by law," open-ended timelines, or the covered entity left holding notification and credit-monitoring cost.
- ☐ **Data ownership and return** SaaS / MSA **Require:** your data stays yours, is used only to deliver the service, and is returned or destroyed in a usable format at exit.
  Watch for: vendor rights to use, aggregate, or de-identify your data for its own purposes — or hostage-data terms and fees to get it back.

Federal healthcare compliance

- ☐ **Healthcare-law compliance and regulatory change** ALL **Require:** compliance with HIPAA, HITECH, and applicable healthcare laws, and a right to reform or exit if the law changes.
  Watch for: a generic "comply with all laws" with no healthcare specificity and no exit when the deal becomes non-compliant.
- ☐ **Exclusion and debarment screening** SERVICES / STAFFING **Require:** a representation that the vendor and its personnel are not excluded (OIG LEIE) or debarred (SAM), screened on an ongoing basis.
  Watch for: no exclusion representation, or a one-time check — a single excluded person can taint every claim the arrangement touches.
- ☐ **Fair market value and referrals** SERVICES / CONSULTING / LEASE **Require:** compensation set at fair market value, commercially reasonable, and not tied to the volume or value of referrals (Stark / Anti-Kickback).
  Watch for: pricing that moves with referrals or volume, or terms that read as payment for patient steering.
- ☐ **Records access and whistleblower rights** SERVICES / MSA **Require:** the Medicare books-and-records access clause where the threshold applies, and no waiver of qui tam or whistleblower rights.
  Watch for: a missing access clause on a reimbursable deal, or a qui tam waiver and confidentiality terms that chill required reporting.

The risk you take on

- ☐ **Indemnification** ALL **Require:** the vendor indemnifies you for its own acts, its IP infringement, and any PHI or data breach it causes.
  Watch for: a one-way indemnity running only from you, or one that quietly excludes data-breach and HIPAA-related claims.
- ☐ **Limitation of liability** ALL **Require:** data-breach, HIPAA, confidentiality, and IP-infringement losses carved out of the liability cap.
  Watch for: a low cap — often one year of fees — that swallows breach exposure, or a consequential-damages waiver that guts your recovery.
- ☐ **Insurance** ALL **Require:** cyber and privacy liability plus general and professional liability, at limits fit to the data and services, with proof on request.
  Watch for: no cyber coverage on a vendor that touches PHI, or limits far below your actual exposure.
- ☐ **Warranties, quality, and recall** GOODS / SaaS / SERVICES **Require:** services to a professional standard; goods that conform to spec and are fit for clinical use; and prompt recall or withdrawal support for defective products.
  Watch for: a blanket "AS IS" disclaimer of merchantability and fitness, or no recall obligation, on products used in patient care.

Continuity, exit, and oversight

- ☐ **Business continuity and disaster recovery** SaaS / SERVICES **Require:** a tested BC/DR plan with committed recovery objectives — downtime on a clinical system reaches patient care.
  Watch for: no committed RTO/RPO, or "best efforts" restoration on a system your clinicians depend on.
- ☐ **Audit and inspection rights** ALL **Require:** the right to audit the vendor's security, compliance, and the records tied to your data and payments.
  Watch for: no audit right, or one so narrow it can't verify HIPAA safeguards or billing compliance.
- ☐ **Termination for cause and transition** ALL **Require:** termination for breach with cure and for insolvency, plus transition help so a switch doesn't strand you.
  Watch for: long cure periods on security failures, or no wind-down help when you need to move.

LegalSifter, Inc. is not a law firm and does not provide legal or compliance advice. Confirm positions with your counsel and compliance team.