ClinicOps

FREE CHECKLIST

Vendor Contract Review Checklist

One checklist for every service, software and supply contract, a one-page register that catches every renewal deadline, and a score in dollars.

Run this checklist on every new vendor contract and again 90 days before each renewal: pages 2 to 4 the review and what goes wrong, page 5 the red flags and a non-renewal notice, page 6 the contract register, page 7 your score. For service, software, maintenance and supply contracts. Real estate leases and employment agreements need an attorney from the start.

48%
of breaches involved a third party in the 2026 report, up from 30% a year earlier and 15% before that
Verizon DBIR 2026, vendor research

32%
of health care fraud cases involved fake or inflated invoices, against 21% of all cases
ACFE, Occupational Fraud 2026

60 days
outer limit for a vendor to tell you about a breach of your patient data; ask for days, not weeks
45 CFR 164.410(b)

Start here: set it up in 20 minutes

1. Fill the register first (page 6): every vendor you paid in the last 12 months, from bank and card statements. One row per contract.
2. Work out each notice deadline: the renewal date minus the notice days. Put it on two calendars, with a reminder 30 days earlier.
3. Run pages 2 to 4 on the next contract to renew and on every new one. Score the register on page 7 every quarter at the staff meeting.

Who signs what

Contract	Reviews	Signs	Before signing
Routine service or supply under the owner's dollar limit	Office manager	Office manager	Blocks 1 to 4 and 8
Over the limit, or longer than 12 months	Office manager	Owner	All eight blocks
Any vendor that creates, receives, keeps or sends patient data	Privacy officer	Owner	All eight blocks; the BAA tracker row
Anything you do not understand, or a vendor that will not change a red flag	Attorney	Owner	Written advice on the marked lines

ClinicOps recommendation. The person who signs a contract should not be the person who approves its invoices (see the internal controls checklist). These pages hold no patient information and never should.

The review, part 1: before you read, term, price

Vendor ref	Service	Cost per year ($)	Reviewer and date

Renewal date	Notice days	Notice deadline	Approver

BLOCK 1: BEFORE YOU READ THE CONTRACT

- [ ] **Every document collected: order form, master agreement, business associate agreement, terms at a web address.**
  Save a dated PDF of any web terms you accept.
- [ ] **Vendor checked against the OIG exclusion list; date written here: _____**
  The free OIG exclusion check on clinicops.us shows how and logs it.
- [ ] **W-9 received before the first payment.**
  IRS: a 1099-NEC is required for nonemployee pay of $2,000 or more to a non-corporate vendor, tax years beginning after 2025.
- [ ] **Nobody in the practice is related to, owns part of, or receives anything from the vendor.**
  ACFE 2026: corruption, which includes conflicts of interest, was in 44% of health care fraud cases.

BLOCK 2: TERM AND RENEWAL

- [ ] **Renewal of one year or less, or month to month after the first term.**
- [ ] **Auto-renewal: the notice deadline is in the register and on two calendars, with a reminder 30 days earlier.**
  Notice deadline = renewal date minus notice days.
- [ ] **How notice must be given, and to which address. Keep proof it arrived.**
- [ ] **New York practices: service, maintenance or repair contracts.**
  NY General Obligations Law 5-903: the renewal is unenforceable unless the vendor reminds you in writing 15 to 30 days before your notice deadline; renewal periods of one month or less are exempt.

BLOCK 3: PRICE AND PAYMENT TERMS

- [ ] **Every fee listed: setup, per user or per provider, per minute or message, support, training, data export, ending the contract.**
  MGMA (Dec 2024): check implementation, customization, support and upgrade costs before you sign.
- [ ] **Price increases at renewal capped at a stated percent, with written notice.**
  'Then-current list price' with no cap lets the vendor set next year's price.
- [ ] **Invoice timing, due date and disputed invoices written down; payment by invoice or a practice card, never open-ended bank debits.**
  One person approves, another pays.
- [ ] **Each invoice will be matched to the contract price before it is paid.**
  ACFE 2026: fake or inflated invoices in 32% of health care fraud cases.

The review, part 2: service, data and privacy

BLOCK 4: SERVICE LEVELS AND SUPPORT

- [ ] **Uptime for software and phones is a number, with a credit when the vendor misses it.**
- [ ] **Support hours span your clinic hours, with a named contact and a response time for an outage that stops patient care.**
- [ ] **On-site vendors: schedule, who enters the building, keys, alarm codes and sign-in.**
  45 CFR 164.310(a): facility access controls.
- [ ] **Copiers, scanners and laptops: the drive is wiped or handed back before the device leaves.**
  45 CFR 164.310(d)(2)(i) and (ii): disposal and media re-use.

BLOCK 5: YOUR DATA AND THE EXIT

- [ ] **The contract says the practice owns its data.**
- [ ] **Export: named format, fee, days to deliver, every record type. For a certified EHR, the full patient population export.**
  45 CFR 170.315(b)(10)(ii): certified EHRs must be able to export all the electronic health information they hold.
- [ ] **You can end for cause without a fee, and for convenience with notice; any early termination fee is a stated amount.**
  45 CFR 164.504(e)(2)(iii): the BAA must let you end it if the vendor violates a material term.
- [ ] **After the exit, patient data is returned or destroyed, with written confirmation.**
  45 CFR 164.504(e)(2)(ii)(J), where feasible.
- [ ] **Transition help for 30 to 90 days after notice, at the same price.**
  Our advice.

BLOCK 6: PATIENT PRIVACY AND SECURITY (ONLY IF THE VENDOR HANDLES PATIENT DATA)

- [ ] **Business associate agreement signed before any patient data moves.**
  45 CFR 164.502(e) and 164.308(b): documented in a written contract.
- [ ] **Subcontractors (hosting, support, AI models) bound to the same terms.**
  45 CFR 164.504(e)(2)(ii)(D); 164.314(a)(2)(i)(B).
- [ ] **Breaches and security incidents reported to you within days.**
  Outer limit: 60 calendar days after discovery, 164.410(b).
- [ ] **MFA on every account that reaches patient data, the vendor's staff included.**
  Verizon DBIR 2026: only 23% of third-party organizations fully fixed missing or weak MFA on cloud accounts.
- [ ] **No use of your data, even with identifiers removed, to train products or for anything the contract does not allow.**
  164.504(e)(2)(i): the contract sets the permitted uses.
- [ ] **Vendor added to the business associate agreement tracker.**
  The free BAA tracker checks the 12 required terms.

The review, part 3: fine print and sign-off

BLOCK 7: LIABILITY, ASSIGNMENT AND THE FINE PRINT

- [ ] **Liability cap at least 12 months of fees; breaches the vendor causes outside the cap or under a higher one.**
  Our advice.
- [ ] **Vendor answers for losses and lawsuits caused by its own breach of the agreement or of the law.**
- [ ] **No assignment to a buyer without notice and your right to leave without a fee.**
- [ ] **Online terms frozen at signing; your state's law governs.**
- [ ] **The person signing has written authority for this contract.**

BLOCK 8: SIGN-OFF

Decision (sign, negotiate, walk away)	Lines to change	Reviewer initials	Approver initials	Filed and in register

Keep signed agreements 6 years from the date they were last in effect (45 CFR 164.316(b)(2)(i), 164.530(j)).

When the review goes wrong

When this happens	Do this
The vendor will handle patient data but will not sign a business associate agreement	Send it no patient data. Use a vendor, or a plan of the same product, that signs one. BAA tracker.
The notice deadline already passed	Reread the clause: some allow ending for convenience with a stated fee. In New York, a service renewal is unenforceable without the 15 to 30 day reminder. Ask for a one-year renewal in place of a long one.
The terms are a click-through that may change at any time	Save a dated PDF of what you accepted. Ask for an order form that fixes the version, or the right to leave without a fee when terms change.
The vendor is bought by another company	Run blocks 5 and 6 again. A new legal entity needs a new business associate agreement; the assignment clause decides whether you can leave.
A staff member signed without authority	Review the contract as if unsigned, negotiate what you can, and write signing limits into policy.
The vendor shuts the product down or stops answering	Ask for the export in writing the same day and set a date. If patient data may have been exposed, start the breach response checklist.
An invoice does not match the contract	Do not pay the difference. Ask the vendor in writing to correct it, and check the last 12 months of invoices from the same vendor.

Red-flag clauses, and what to ask for instead

When the contract says	Ask for
Renews automatically for successive terms equal to the initial term	Renewal of one year at most, or month to month after the first term
Notice of non-renewal at least 90 days before the end of the term	30 days' notice by email to a named address, plus a written reminder from the vendor before the deadline
Fees may increase to the vendor's then-current list price	Increases capped at a stated percent a year, with 60 days' written notice
Customer authorizes automatic debits from its bank account	Invoice or card payment; any debit limited to the contract amount
Vendor will use commercially reasonable efforts to maintain availability	Uptime of a stated percent, with a credit when missed
Data export available at vendor's then-current professional services rates	A complete export in a named format within a set number of days, at a stated fee or free
Vendor may modify these terms by posting a revised version	Changes only with your written agreement, or the right to leave without a fee
Vendor's total liability shall not exceed fees paid in the prior month	At least 12 months of fees; privacy breaches the vendor causes outside or above the cap
Vendor may assign this agreement without consent	Written notice of any assignment and the right to end the contract without a fee
Vendor may use customer data to improve its services	Use only to serve the practice, as the business associate agreement permits; no training on your data

The non-renewal notice

Send it the way the contract's notice clause says, before the notice deadline, and file the proof. Replace each blank.

Notice of non-renewal

To: _____ (vendor, at the notice address in the contract). Re: agreement _____ dated _____. [Practice name] gives notice under section ____ of the agreement that it will not renew the agreement when the current term ends on _____. Please confirm receipt in writing within 5 business days, deliver a complete export of our data in _____ format by _____ as section ____ provides, and confirm in writing when all patient information has been returned or destroyed. [Name, title, date].

Sent on	Sent how	Proof filed at	Vendor confirmed on

The contract register

One row per contract, sorted by notice deadline. The office manager reads it on the first working day of each month and the owner sees it every quarter. Notice deadline = renewal date minus notice days. Reference codes or vendor names only: no patient information.

Ref	Service	Per year ($)	Auto Y/N	Patient data / BAA	Renews on	Notice days	Notice deadline	Owner
V-01	EHR and practice software	28,800	Y	Yes / signed	Mar 1, 2027	90	Dec 1, 2026	Office mgr
V-02	Phone system	9,600	Y	Yes / signed	Feb 15, 2027	90	Nov 17, 2026	Office mgr

The two filled rows are from the worked example on page 7. Delete them or write over them. The phone contract's deadline passed two days before this file's date, which is exactly what the register is for.

Your vendor exposure score

Worked example: a 3-physician family practice with 11 vendor contracts. Illustrative numbers, not a client. Fill the Yours column from your register each quarter.

Line	How to work it out	Worked example	Yours
A. Contracts on the register	Count of rows	11	
B. Spend under contract, per year	Sum of Per year	$96,400	
C. Spend that renews automatically	Sum where Auto = Y	$71,200	
D. Spend on autopilot	Part of C with no notice deadline on two calendars	$36,400	
E. Share on autopilot	D / B	38%	
F. Biggest lock-in a missed deadline would cause	Per year x renewal years, worst contract	$28,800	
G. Next year's unreviewed increase	D x the increase your vendors gave last year (example 6%)	$2,184	
H. Vendors that handle patient data	Count	8	
I. Of those, no signed business associate agreement	Count	2	
J. Contracts with no data export clause	Count	3	
K. Invoices paid last month without a contract match	Count, from the bank and card statements	5 of 14	

Lines D to G are a ClinicOps calculation from your own entries. For scale: fake or inflated invoices had a median loss of $90,000 across all 2,402 cases in the ACFE's 2026 study, and appeared in 28% of cases at organizations with fewer than 100 employees.

Read your grade

Holding	I is 0, E under 10%, J 1 or fewer	Keep the monthly register read; run the checklist at every renewal.
Slipping	I is 0, but E is 10% to 25% or J is 2 or more	Put every deadline on two calendars this month; fix the exit clauses at each renewal.
Exposed	I is 1 or more, or E over 25%	Stop sending patient data to vendors without an agreement, then work the deadlines from the soonest.

Grades are ClinicOps thresholds, not a legal standard. The worked example scores Exposed: two vendors handle patient data with no agreement, and 38% of spend renews on autopilot.

The full guide, with the rule behind each line and the vendors that need which checks: the vendor contract review checklist on clinicops.us. For the business associate agreement itself, use the free BAA tracker.

Sources

Every figure and rule here was checked against the original source on Nov 19, 2026. Rules and figures change: confirm anything time-sensitive on the source page.

1. Verizon, 2026 Data Breach Investigations Report: third-party involvement 48% (30% prior year); healthcare 32% of 1,438 breaches; 23% MFA remediation (2026 edition, incidents Nov 1, 2024 to Oct 31, 2025). verizon.com/business/resources/Tbe7/reports/2026-dbir-data-breach-investigations

2. Verizon, 2025 DBIR: third-party involvement doubled from 15% to 30% (2025). verizon.com/business/resources/Tbe7/reports/2025-dbir-data-breach-investigations

3. ACFE, Occupational Fraud 2026: A Report to the Nations: invoice schemes 32% of health care cases, 21% of all, median loss $90,000; corruption 44%; by size 28% vs 18% (2026). acfe.com/-/media/files/acfe/pdfs/rttn/2026/2026-report-to-the-nations.pdf

4. MGMA Stat poll: 40% have a clear process to select new technology; buyer checklist (Dec 10, 2024). mgma.com/mgma-stat/selecting-new-technology-starts-with-a-clear-process-to-evalu

5. 45 CFR 164.502(e), 164.504(e), 164.308(b), 164.314(a): business associate contracts (eCFR, current to Nov 16, 2026). ecfr.gov/current/title-45/section-164.504

6. 45 CFR 164.410(b): business associate breach notice, 60 calendar days (eCFR, current to Nov 16, 2026). ecfr.gov/current/title-45/section-164.410

7. 45 CFR 164.310(a) and (d): facility access, disposal and media re-use; 164.316(b)(2)(i) and 164.530(j): 6-year retention (eCFR, current to Nov 16, 2026). ecfr.gov/current/title-45/section-164.316

8. 45 CFR 170.315(b)(10): electronic health information export from certified health IT (eCFR, current to Nov 16, 2026). ecfr.gov/current/title-45/section-170.315

9. New York General Obligations Law 5-903: automatic renewal of service, maintenance or repair contracts (current). nysenate.gov/legislation/laws/GOB/5-903

10. IRS, Instructions for Forms 1099-MISC and 1099-NEC: $2,000 threshold for tax years beginning after 2025 (Rev. December 2026). irs.gov/instructions/i1099mec

Where this checklist stops

The checklist makes every signature a reviewed one. Here is what paper cannot do on its own:

- **It cannot read a renewal notice for you: it works only if a named person reads the register every month.**
- **It cannot negotiate. The asks on page 5 work only when someone sends them before the deadline.**
- **It is not legal advice. A contract you do not understand, or a vendor that will not move on a red flag, goes to your attorney.**

Practice Controls, part of Fix one system: we build the contract register, renewal reminders and signing limits, together with the SOP library, the recurring task board and the compliance calendar, inside the tools you already use, then hand it over.

Book the free 20-minute Chaos Audit >

It is a diagnostic call, not a sales call: we walk back the last thing that slipped, put an hours or dollar figure on it, and you leave with the first fix whether or not you hire us.

Not ready to talk? Score your practice in 3 minutes, or get more free tools and templates.
Follow ClinicOps for one useful fix a week: LinkedIn | YouTube | X | Instagram | Facebook