ClinicOps

FREE CHECKLIST

Microsoft 365 HIPAA Setup Checklist

34 checks in setup order, a score that sizes your gaps in points and hours, a filled example, and what to do when something goes wrong.

Run this with whoever administers your Microsoft 365 tenant: about an hour the first time, 20 minutes each quarter after that. Tick what is true today, score what is not, and fix in the order the score gives you.

99.2%
of identity-based attacks blocked by multifactor sign-in, per Microsoft
Microsoft Learn, 2026 (vendor figure)

180 days
how long Audit (Standard) keeps records in every business plan
Microsoft Learn, 2026

$3 million
paid to HHS by Solara Medical Supplies after a phishing breach
HHS OCR, Jan 14, 2025

6 years
how long HIPAA documentation must be kept
45 CFR 164.316

Start here

1. Fill in the lines below, then work through the 34 checks on pages 2 to 4 with your admin. Tick only what you can show on screen today.
2. Score the gaps on page 4. Each unticked check carries points (5 critical, 3 important, 1 good practice) and minutes to fix, shown on its row.
3. Fix in score order: every 5-point gap first, then 3, then 1. The worked example on page 5 shows a finished score and the first three fixes.
4. Re-score every quarter and after any staff change. The reasons behind each check are in the Microsoft 365 HIPAA guide on clinicops.us.

Practice: _____

Tenant admin (name): _____

Plan and license count: _____

Date of this review: _____

DPA version on file: _____

Next review date: _____

Privacy note
This checklist holds no patient information and needs none: never write a patient name, chart number or date on it. Microsoft says using its services does not on its own achieve HIPAA compliance; your plan, settings and policies decide that. This is an operations checklist, not legal advice.

Version 1.0, Nov 18, 2026. Every fact checked at its source on Nov 17, 2026; Microsoft changes plans and settings often, so re-check the source pages listed at the end.

The 34 checks, in setup order

Pts = points if NOT done. Min = minutes to fix, our estimate for a 1 to 10 user tenant. Plan = All business plans, or Business Premium only.

A. Agreement and plan

	Pts	Min	Plan
☐ **1. Everyone who handles patient information works in a Microsoft 365 business plan account. No Personal, Family or personal Outlook.com accounts.** The BAA reaches business subscriptions through Microsoft's Data Protection Addendum (Microsoft Learn, 2026).	5	30	All
☐ **2. The current Data Protection Addendum is saved with your compliance records (the November 2026 version on Nov 17, 2026).** It is the document that carries Microsoft's BAA terms.	3	10	All
☐ **3. A dated copy of Microsoft's HIPAA in-scope service list is saved next to it.** Proves what was covered when you decided.	1	5	All
☐ **4. Microsoft is logged in your BAA tracker with the DPA date and a yearly review date.** HIPAA documentation is kept 6 years (45 CFR 164.316).	1	5	All
☐ **5. No patient information sits in apps missing from the in-scope list: Bookings, Loop, To Do, Viva, Clipchamp or Shifts.** Bookings ships with every business plan but is not on Microsoft's HIPAA list.	5	30	All

B. Sign-in

	Pts	Min	Plan
☐ **6. Security defaults are on, or Conditional Access requires multifactor sign-in for every user.** Conditional Access needs Entra ID P1, included in Business Premium.	5	20	All
☐ **7. Every user has finished multifactor registration.** Microsoft removed the 14-day registration grace period on July 29, 2024.	3	15	All
☐ **8. Legacy authentication is blocked. Printers and scan-to-email devices were checked first.** Old protocols cannot do multifactor sign-in.	3	20	All
☐ **9. Admins use separate admin accounts, never their daily login.** Microsoft's advice on the security defaults page.	3	15	All
☐ **10. Two cloud-only emergency access accounts exist, with credentials stored offline.** Microsoft recommends two for lock-out scenarios.	1	15	All
☐ **11. One named account per person, including the front desk. No shared logins.** Unique user identification is required (45 CFR 164.312(a)(2)(i)).	3	30	All

C. Email

	Pts	Min	Plan
☐ **12. Automatic external forwarding is set to Off, not Automatic, in the outbound spam policy.** Microsoft advises On or Off, because Automatic behaves differently by tenant age.	5	10	All
☐ **13. Inbox rules that forward outside the practice were reviewed this quarter.** A phished mailbox often gets a hidden forwarding rule.	3	15	All
☐ **14. Staff have a written rule for emailing patient information outside the practice: who may, to whom, and only what is needed.** Your policy, enforced by training.	3	20	All

☐	**15. A data loss prevention policy warns or blocks when patient identifiers leave by email.** Premium includes Purview DLP for email and files.	3	30	Premium
☐	**16. Defender for Office 365 Plan 1 protections are switched on and reviewed.** Premium includes Plan 1; Basic and Standard get time-of-click URL protection.	1	20	Premium

D. Files, sharing and Teams

		Pts	Min	Plan
☐	**17. SharePoint external sharing is New and existing guests or stricter. Never Anyone.** Anyone links open files without sign-in (Microsoft Learn, 2026).	5	10	All
☐	**18. OneDrive sharing is the same as SharePoint or stricter.** OneDrive can be stricter than SharePoint, never looser.	3	5	All
☐	**19. The default sharing link is Specific people.** Staff take the default most of the time.	3	5	All
☐	**20. Guest access expires automatically after a set number of days.** Old guests are the forgotten doors.	1	5	All
☐	**21. Teams guests and external access are limited to named partners and reviewed each quarter.** A former contractor in a team still sees its files.	3	20	All
☐	**22. A written rule says when Teams meetings may be recorded or transcribed, and who may see recordings.** Recordings with patient details are PHI.	3	20	All

On Business Basic or Standard?

Checks 15, 16 and 25 to 27 need Business Premium. Tick one only if your risk analysis documents another control that covers the same risk, such as another endpoint tool. Otherwise score it as a gap: it is a real one.

E. Devices

		Pts	Min	Plan
☐	**23. Every laptop and phone that opens work email has a passcode and a screen lock.** Automatic logoff is an addressable safeguard (45 CFR 164.312(a)(2)(iii)).	5	30	All
☐	**24. Every practice laptop is encrypted (BitLocker or FileVault) and your risk analysis records it.** Encryption is addressable (164.312(a)(2)(iv)); encrypted PHI is not unsecured PHI (164.402).	5	30	All
☐	**25. Practice laptops and phones are enrolled in Intune.** Premium includes Intune Plan 1.	3	60	Premium
☐	**26. A lost device can be wiped remotely, and the steps are written down.** Needs device management.	3	15	Premium
☐	**27. Defender for Business is on for every practice computer.** Premium includes it.	3	30	Premium

F. Watching and people

		Pts	Min	Plan
☐	**28. Someone searches the Purview audit log every month for sign-ins, mailbox rules and sharing.** Audit (Standard) is on by default in every business plan.	3	20	All
☐	**29. Audit records you need beyond 180 days are exported and stored.** Audit (Standard) keeps records 180 days.	1	15	All

☐	**30. Departures: sign-in blocked, sessions revoked, forwarding removed and devices wiped the same day.** Most leaks after a departure come from accounts left open.	5	15	All
☐	**31. A quarterly access review checks admins, guests, shared mailboxes and licenses.** Access is granted fast and removed slowly.	3	30	All
☐	**32. Microsoft 365 is listed in your security risk analysis with its plan, DPA date and settings.** Risk analysis is required (45 CFR 164.308(a)(1)(ii)(A)).	5	60	All
☐	**33. Staff were trained on phishing and the email rule in the last 12 months, with attendance recorded.** Security awareness training is required (45 CFR 164.308(a)(5)).	3	45	All
☐	**34. The settings and decisions above are written down and kept 6 years.** 45 CFR 164.316(b)(2)(i).	1	20	All

Your exposure score

For each section, add up the points and minutes of every check you did not tick. Type the numbers into the boxes or write them in. The most a tenant can score is 106 points.

Section	Points possible	Your points (not done)	Your minutes to fix	Minutes if nothing is done
A. Agreement and plan	15			80
B. Sign-in	18			115
C. Email	15			95
D. Files, sharing and Teams	18			65
E. Devices	19			165
F. Watching and people	21			205
Total	**106**			**725**

Your total	What it means	What to do
0 to 10	Tidy. The basics are in place.	Close the 1-point gaps this quarter and re-score after staff changes.
11 to 30	Exposed. At least one door is open.	Close every 5-point gap this month, starting with forwarding, sharing and departures.
31 or more	High risk. A phished mailbox or a lost phone would likely become a reportable breach.	Close the 5-point gaps this week. Divide your minutes by 60 for the hours to book with your admin.

Worked example: a seven-user practice on Business Standard

A composite, not a client: a two-physician family practice, seven users, one outside IT contact. The office manager and the admin ran the checklist in 70 minutes.

Section	Gaps found (check number)	Points	Minutes
A. Agreement and plan	Bookings used for new-patient requests (5)	5	30
B. Sign-in	Office manager's daily login is a Global Administrator (9); no emergency access accounts (10)	4	30
C. Email	Forwarding left on Automatic (12); no DLP (15) or Defender for Office 365 Plan 1 (16) on Standard, no documented alternative	9	60
D. Files, sharing and Teams	SharePoint set to Anyone (17); guest access never expires (20)	6	15
E. Devices	No device management on Standard (25, 26); check 27 ticked because the IT contact runs another endpoint tool, documented in the risk analysis	6	75
F. Watching and people	Audit log never searched (28); nothing exported (29); Microsoft 365 missing from the risk analysis (32)	9	95
Total	12 gaps	39: high risk	305 (about 5 hours)

First three fixes, in order: forwarding to Off (10 minutes), SharePoint to New and existing guests (10 minutes), and patient requests moved from Bookings to the EHR's scheduling (30 minutes). Those 50 minutes take the score from 39 to 24: exposed, not high risk. Moving to Business Premium (seven users x $8 more per user per month = $672 a year at Microsoft's Nov 2026 list prices) makes checks 15, 16, 25 and 26 possible, worth 10 more points once they are switched on.

What one gap can cost: HIPAA civil money penalties

Per violation, 45 CFR 102.3 as adjusted, current on eCFR Nov 13, 2026.

Culpability	Minimum	Maximum	Yearly cap
Did not know, and could not have known	$145	$73,011	$2,190,294
Reasonable cause, not willful neglect	$1,461	$73,011	$2,190,294
Willful neglect, corrected within 30 days	$14,602	$73,011	$2,190,294
Willful neglect, not corrected	$73,011	$2,190,294	$2,190,294

Phishing cases on HHS's resolution agreements list: Solara Medical Supplies $3,000,000 (Jan 14, 2025); a health care network $600,000 (Apr 23, 2025); Ambry Genetics $700,000 (Sep 17, 2026).

When it goes wrong: the playbook

The unusual cases are where practices get hurt. Work the row, then tell your privacy officer the same day. Breach notice duties run from the day of discovery.

When this happens	Do this	The rule behind it
An email with patient information went to the wrong outside address	Ask the recipient to delete it and confirm in writing. Tell the privacy officer today. Run the four-factor risk assessment and keep it.	Presumed a breach unless a low probability of compromise is shown (45 CFR 164.402)
A staff phone or laptop with work email is lost	Block sign-in and revoke sessions. Wipe it if it is enrolled. Record whether it was encrypted and locked.	Encrypted PHI is not unsecured PHI (164.402); notify within 60 days if it is a breach (164.404)
A mailbox was phished	Block sign-in, reset the password, revoke sessions, delete forwarding and inbox rules, then search the audit log for what the attacker touched.	Audit (Standard) keeps 180 days: search now, export what you find
A leaver's mail is still forwarding or syncing	Block sign-in, remove forwarding, wipe the device, and check the audit log for what left after the last day.	Unique user identification and access control (164.312(a))
Staff set up Bookings for patient requests	Stop collecting patient details there. Move requests to the EHR or portal and record the change in the risk analysis.	Bookings is not on Microsoft's HIPAA in-scope list
Patient files went out from a personal Outlook.com or Gmail account	Treat it as a possible breach and assess it. Move the person to a work account and retrain.	Personal accounts sit outside Microsoft's DPA and BAA
An Anyone link to a file with patient data was shared	Stop sharing the link, check who opened it in the audit log, and assess the exposure.	Same four-factor test (164.402)
A Teams recording with patient details reached a guest	Remove the guest, restrict or delete the recording under your retention rule, and assess.	Your written recording rule (check 22)
An outside IT company needs admin access	Sign a BAA with them first, then give a named admin account. Never share a login.	BA assurances first (164.308(b)(1), 164.504(e))
A patient emails asking for their records	Log the date received and act within 30 days (15 days from July 17, 2027, under the HHS final rule filed Nov 16, 2026). Send through your EHR or portal, or by email if the patient asks for it.	Right of access (45 CFR 164.524(b)(2))

Where to go next

Log every vendor agreement, not just Microsoft, in the free business associate agreement tracker. The plan-by-plan detail, prices and settings paths are in the Microsoft 365 HIPAA setup guide.

Sources

Checked against the original source in November 2026. Rules and figures change: confirm anything time-sensitive on the source page.

1. Microsoft Learn: HIPAA and HITECH Act offering, BAA through the DPA, in-scope services (updated Sep 11, 2026).
learn.microsoft.com/en-us/compliance/regulatory/offering-hipaa-hitech

2. Microsoft: Products and Services Data Protection Addendum, version list (November 2026 version).
microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protect

3. Microsoft: Microsoft 365 business plans with Teams, prices and compare table (Nov 17, 2026).
microsoft.com/en-us/microsoft-365/business/with-teams-plans-and-pricing

4. Microsoft Learn: Security defaults in Microsoft Entra ID (updated Oct 16, 2026).
learn.microsoft.com/en-us/entra/fundamentals/security-defaults

5. Microsoft Learn: Auditing solutions in Microsoft Purview (180-day retention) (updated Jul 8, 2026).
learn.microsoft.com/en-us/purview/audit-solutions-overview

6. Microsoft Learn: Manage sharing settings for SharePoint and OneDrive (Jun 30, 2026).
learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

7. Microsoft Learn: Control external email forwarding (Aug 18, 2026).
learn.microsoft.com/en-us/defender-office-365/outbound-spam-policies-external-

8. HHS OCR: Resolution agreements and civil money penalties (reviewed Oct 30, 2026).
hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

9. 45 CFR 102.3: civil money penalty amounts, as adjusted (eCFR, Nov 13, 2026).
ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-102/section-102.3

10. 45 CFR 164.308, 164.312, 164.316: administrative and technical safeguards, documentation (eCFR, Nov 13, 2026).
ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C

11. 45 CFR 164.402, 164.404: breach definition and notice to individuals (eCFR, Nov 13, 2026).
ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D

12. 45 CFR 164.504(e), 164.524: business associate contracts, right of access (eCFR, Nov 13, 2026).
ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E

Where this checklist stops

It shows you where the gaps are and what each one weighs. Closing them, and keeping them closed when staff change, is the work.

- **It cannot switch a setting on, see your tenant, or notice the day a new hire is made a Global Administrator.**
- **It cannot tell you whether a misdirected email is a reportable breach: your privacy officer and counsel decide that.**
- **It does not train your staff or run the quarterly review for you.**
- **It covers Microsoft 365 only, not your EHR, phones, fax or website.**

Practice Controls: an SOP library a new hire can run on day one, a recurring task board, license and compliance calendars, and the cash controls that stop leakage.

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