



Home Health IT and HIPAA Readiness Checklist

47 plain questions for a California home health agency. Fifteen minutes, a pen, and honest answers will show you where your technology and your HIPAA paperwork stand today.

1. Answer each question

Tick Yes only if you could show it to a surveyor today. If you are not sure, tick Unsure. Unsure counts as No.

2. Count your No and Unsure

Add them up at the end and read the guide on the last page.

3. Fix the stars first

The 13 items marked ★ are the ones that do the most to reduce risk for a small agency.

★ Fix first · Citations point to 45 CFR Part 164, the HIPAA Security, Privacy and Breach Notification Rules.

Sign-in and access

	YES	NO	UNSURE	
1	☐	☐	☐	Every person has their own sign-in. There are no shared logins or shared passwords. 45 CFR 164.312(a)(2)(i)
2	☐	☐	☐	★ Multi-factor sign-in is on for every account, administrators first. 45 CFR 164.312(d)
3	☐	☐	☐	★ Accounts for people who have left are disabled the same day. 45 CFR 164.308(a)(3)(ii)(C)
4	☐	☐	☐	Administrators use a separate account for admin work, not their everyday one.
5	☐	☐	☐	People can open only the folders and systems their job needs. 45 CFR 164.308(a)(4)
6	☐	☐	☐	Guest and outside accounts (contractors, field staff on personal email) are reviewed at least every quarter.
7	☐	☐	☐	Someone reviews who has access to the EMR at least twice a year. 45 CFR 164.308(a)(4)

Computers and phones

	YES	NO	UNSURE	
8	☐	☐	☐	★ Every laptop and phone that touches PHI is encrypted. 45 CFR 164.312(a)(2)(iv)
9	☐	☐	☐	Screens lock automatically after a few minutes of inactivity. 45 CFR 164.312(a)(2)(iii)
10	☐	☐	☐	A lost or stolen device can be locked and wiped remotely.
11	☐	☐	☐	★ Updates install automatically, and nothing runs a version of Windows that Microsoft no longer supports.
12	☐	☐	☐	Every device has current antivirus or endpoint protection that staff cannot switch off.
13	☐	☐	☐	You keep a list of every device that touches PHI and who has it. 45 CFR 164.310(d)(1)

Email and messages

	YES	NO	UNSURE	
14	☐	☐	☐	Your email domain has SPF, DKIM and DMARC records, so it is hard to fake your address.
15	☐	☐	☐	Email filtering blocks phishing messages and dangerous attachments.
16	☐	☐	☐	Staff know not to send PHI in ordinary email or text messages, and have an approved way to share it. 45 CFR 164.312(e)(1)
17	☐	☐	☐	Any change to bank or payment details is confirmed by a phone call to a known number.
18	☐	☐	☐	Automatic forwarding of mail to outside addresses is blocked or reviewed.

Network and Wi-Fi

	YES	NO	UNSURE	
19	☐	☐	☐	★ A business-grade firewall is in place, with current firmware and logging switched on.
20	☐	☐	☐	Guest Wi-Fi is on a separate network from staff devices and systems.
21	☐	☐	☐	★ No remote-desktop or admin ports are open to the internet, and remote access needs multi-factor sign-in.
22	☐	☐	☐	Printers, scanners and phones are on their own network segment, with default passwords changed.
23	☐	☐	☐	Someone scans for known vulnerabilities at least quarterly and fixes what they find. 45 CFR 164.308(a)(1)(ii)(A)-(B)

Backup and recovery

	YES	NO	UNSURE	
24	☐	☐	☐	★ Microsoft 365 mail and files have a separate backup. Microsoft's own retention is not a backup. 45 CFR 164.308(a)(7)(ii)(A)
25	☐	☐	☐	★ At least one backup copy cannot be changed or deleted from an ordinary office computer (offline or immutable).
26	☐	☐	☐	★ You have restored something from backup in the last 12 months and know how long it took. 45 CFR 164.308(a)(7)(ii)(D)
27	☐	☐	☐	A written recovery plan says what is restored first and who does it. 45 CFR 164.308(a)(7)(ii)(B)
28	☐	☐	☐	Staff know what to do when the EMR, the internet or the phones are down (paper forms, a call tree). 45 CFR 164.308(a)(7)(ii)(C)
29	☐	☐	☐	The plan and contact list also exist outside your computer systems, printed or on a phone.

Vendors and agreements

	YES	NO	UNSURE	
30	☐	☐	☐	You keep a list of every vendor that can see PHI: EMR, phones, email, billing, shredding, IT, cloud. 45 CFR 164.308(b)
31	☐	☐	☐	★ A signed Business Associate Agreement is on file for each one. 45 CFR 164.308(b); 164.504(e)
32	☐	☐	☐	You know which of each vendor's plans or features the agreement actually covers.
33	☐	☐	☐	Renewal dates and exit terms for major vendors are written down.
34	☐	☐	☐	New tools are approved before staff start using them.

AI and new tools

	YES	NO	UNSURE	
35	☐	☐	☐	You have a written rule for AI tools: what may and may not be put into them.
36	☐	☐	☐	Staff know never to paste PHI into public AI chat tools.
37	☐	☐	☐	Any AI tool that sees PHI runs inside your own Microsoft 365 tenant or on equipment you control, under an agreement.
38	☐	☐	☐	A person checks AI output before it is filed, sent or acted on.

People and training

	YES	NO	UNSURE	
39	☐	☐	☐	Every new hire gets HIPAA and security training before they can reach PHI. 45 CFR 164.308(a)(5); 164.530(b)
40	☐	☐	☐	★ All staff repeat it at least once a year, and you keep a record of who and when. 45 CFR 164.308(a)(5)
41	☐	☐	☐	Staff practice spotting phishing and know whom to tell the moment something looks wrong.
42	☐	☐	☐	A named person is responsible for security, and a named person for privacy. 45 CFR 164.308(a)(2); 164.530(a)

Paperwork you can show a surveyor

	YES	NO	UNSURE	
43	☐	☐	☐	★ A written risk analysis exists and was updated in the last 12 months. 45 CFR 164.308(a)(1)(ii)(A)
44	☐	☐	☐	A risk management plan lists what will be fixed, who owns each item and by when. 45 CFR 164.308(a)(1)(ii)(B)
45	☐	☐	☐	Audit logging is on for email, the EMR and file storage, and someone looks at it. 45 CFR 164.312(b)
46	☐	☐	☐	★ A written incident and breach response plan names who decides and who calls whom. 45 CFR 164.308(a)(6); 164.400-414
47	☐	☐	☐	Policies are reviewed at least yearly and match what staff really do. 45 CFR 164.316(b)

How to read your score

Count every question you answered No or Unsure.

0 to 5	A strong foundation. Keep the evidence current and test what you have.
6 to 15	Some gaps. Work through the starred items first; most are quick to fix.
16 or more	Significant gaps. A long list is a starting point, not a verdict. Start with the starred items and ask for help.

A rough guide for conversation, not a measure of compliance. An agency can answer Yes to everything here and still have gaps, and a No does not by itself mean a violation.

Want help with your No answers?

Algorixtec works with California home health agencies on security, backup, Microsoft 365, HIPAA paperwork and training. Bring this sheet to a free working session and we will turn it into a ranked fix list.

www.algorixtec.com/contact.html · hello@algorixtec.com

This checklist is general guidance for small agencies. It is not legal advice, does not determine whether your agency complies with HIPAA, California law, Medicare requirements or any accreditation standard, and no product or service is "HIPAA certified". Your compliance officer and counsel decide what your agency must do. © Algorixtec LLC. You may share this sheet unchanged.