HIPAA Readiness Checklist

30 questions for small practices, medspas and health-tech teams

Answer **Yes** only if you could show the evidence today: a signed document, a setting you can screenshot, or a record with a date on it. Intentions and verbal agreements count as No. It takes about 15 minutes.

Scope and responsibility

		YES	NO
1	We have confirmed in writing whether we are a HIPAA covered entity, a business associate, or neither.	☐	☐
2	A named person is responsible for privacy and a named person for security. One person can hold both roles.	☐	☐
3	We keep a current list of every system, device and vendor that stores or sends patient information.	☐	☐
4	We know every place patient information leaves our control: labs, pharmacies, billing, marketing and IT support.	☐	☐
5	Leadership has reviewed our privacy and security status in the past 12 months.	☐	☐

Risk analysis and management

		YES	NO
6	We have a written security risk analysis dated within the past 12 months.	☐	☐
7	Each risk in it has a likelihood, an impact and a recorded decision about what we will do.	☐	☐
8	We have a remediation plan with an owner and a target date for each action.	☐	☐
9	We update the risk analysis when we add a location, a system or a new service line.	☐	☐
10	We keep risk analyses, policies and related records for at least six years.	☐	☐

Vendors

		YES	NO
11	Every vendor that handles patient information has a signed business associate agreement where one is required.	☐	☐
12	We check a new vendor's security before staff start using it.	☐	☐
13	Our booking, intake and email tools are covered by a business associate agreement, or hold no health information.	☐	☐
14	When a vendor contract ends, access is removed and our data is returned or destroyed.	☐	☐
15	We know how and how quickly each key vendor would tell us about a breach.	☐	☐

Access and devices

		YES	NO
16	Everyone has their own login. No shared accounts for the EHR, email or e-prescribing.	☐	☐
17	Multi-factor authentication is on for email, the EHR and any remote access.	☐	☐
18	Laptops and phones that hold patient information are encrypted and can be wiped remotely.	☐	☐
19	Access is removed the same day someone leaves, contractors included.	☐	☐

© 2026 Empyric Compliance LLC · hello@empyriccompliance.com

Access and devices

		YES	NO
20	Systems receive security updates automatically or on a set schedule.	☐	☐

People, photos and messaging

		YES	NO
21	Everyone with access, contractors included, completed privacy and security training this year and signed for it.	☐	☐
22	Patient photos are taken and stored on devices or systems we control, not personal phones or accounts.	☐	☐
23	No patient photo or testimonial is used in marketing without a signed authorization.	☐	☐
24	Patients have agreed in writing to how we text or email them.	☐	☐
25	Tracking pixels are kept off booking pages, patient portals and any page behind a login.	☐	☐

Incidents and recovery

		YES	NO
26	We have written steps for a lost device, a misdirected message or a suspected breach.	☐	☐
27	Staff know whom to tell, and how fast, when something goes wrong.	☐	☐
28	We decide whether an incident is a reportable breach using a set process, and we document the decision.	☐	☐
29	Backups are kept separate from our main systems and have been restored in a test this year.	☐	☐
30	If HIPAA applies, our Notice of Privacy Practices is in use and we can answer patient records requests on time.	☐	☐

Your score

26 to 30 Yes	A solid foundation. Keep the risk analysis, training and vendor list current, and re-run this checklist each year.
18 to 25 Yes	Real gaps, often in documentation. Start with items 1, 6, 11 and 17, then work through the rest by section.
Under 18 Yes	Time to build the program. Begin by confirming which rules apply (item 1) and completing a written risk analysis (item 6).

Items 6, 11 and 17 come up first in practice. The HHS Office for Civil Rights asks for the written risk analysis at the start of breach investigations, and cyber insurance applications routinely ask about multi-factor authentication and vendor agreements.

Want a second set of eyes?

Empyric Health Compliance offers one-hour advisory calls and fixed-fee programs, including a 90-minute Coverage and Exposure Check for medspas and wellness clinics. Visit **empyriccompliance.com** or write to **hello@empyriccompliance.com**.

This checklist is general information for self-assessment. It is not legal advice and does not establish compliance with HIPAA, Wisconsin law or any other requirement.