CERTIFY HEALTH

HIPAA-Compliant Patient Communication Self-Assessment

(Score Your Risk in 10 Minutes)

How to use this:

For each question, check Yes if your practice is fully compliant.
If not, leave it unchecked—that's a gap.

1. Communication Visibility Audit

- Do you have a complete list of all patient communication channels used today?

  ☐ Yes ☐ No

- Do you know exactly where PHI is shared across all communication channels?

  ☐ Yes ☐ No

- Have you eliminated the use of personal phones, personal email, or unapproved apps for patient communication?

  ☐ Yes ☐ No

- Does every communication vendor you use provide a signed Business Associate Agreement (BAA)?

  ☐ Yes ☐ No

- Are all your communication channels encrypted both in transit and at rest?

  ☐ Yes ☐ No

- Can you track message activity with audit logs (who sent what, when, and to whom)?

  ☐ Yes ☐ No

2. Everyday Communication Risks

- Avoid sharing PHI on unsecured messages?

  ☐ Yes ☐ No

- Do your voicemail messages avoid mentioning sensitive health details?

  ☐ Yes ☐ No

- Verify patient identity before sharing info?

  ☐ Yes ☐ No

- Are sensitive conversations kept out of public or front-desk areas?

  ☐ Yes ☐ No

- Has your team been trained on the “minimum necessary” rule for PHI?

  ☐ Yes ☐ No

3. Texting & Messaging Compliance

- Have you completely stopped sending PHI through standard SMS or personal devices?

  ☐ Yes ☐ No

- Are all patient messages sent through a secure, encrypted messaging platform?

  ☐ Yes ☐ No

- Does your messaging system maintain complete audit logs for all communications?

  ☐ Yes ☐ No

- Do you separate low-risk messages (reminders) from high-risk ones (labs, diagnoses)?

  ☐ Yes ☐ No

- Are high-risk messages only sent through HIPAA-compliant secure channels?

  ☐ Yes ☐ No

4. Email Compliance

- Does your email provider support HIPAA compliance with a signed BAA?

  ☐ Yes ☐ No

- Is encryption enabled for email both in transit (TLS 1.2+) and at rest?

  ☐ Yes ☐ No

- Are email subject lines free from PHI?

  ☐ Yes ☐ No

- Do you avoid sending detailed clinical information through email?

  ☐ Yes ☐ No

- Do you use email primarily to redirect patients to a secure portal?

  ☐ Yes ☐ No

- Have you documented patient consent for email communication?

  ☐ Yes ☐ No

5. Consent & TCPA Alignment

- Do you collect explicit written consent before sending SMS messages?

  ☐ Yes ☐ No

- Are patients informed about the risks of SMS communication?

  ☐ Yes ☐ No

- Do you provide a clear opt-out option for messaging?

  ☐ Yes ☐ No

- Are patient communication preferences (text, call, email) documented and enforced?

  ☐ Yes ☐ No

- Does your system automatically manage opt-in and opt-out tracking?

  ☐ Yes ☐ No

6. Appointment Reminder Safety

- Do your reminders avoid mentioning sensitive specialties or conditions?

  ☐ Yes ☐ No

- Do you exclude diagnoses, procedures, and clinical details from reminders?

  ☐ Yes ☐ No

- Are reminders limited to date, time, location, and simple instructions?

  ☐ Yes ☐ No

- Do you use neutral, non-revealing language in all reminders?

  ☐ Yes ☐ No

7. Access Control & Internal Security

- Do you use role-based access for staff (front desk vs clinician vs admin)?

  ☐ Yes ☐ No

- Have you eliminated shared logins across your team?

  ☐ Yes ☐ No

- Is multi-factor authentication (MFA) enabled across systems?

  ☐ Yes ☐ No

- Do systems automatically log users out after inactivity?

  ☐ Yes ☐ No

- Can lost or stolen devices be remotely secured or wiped?

  ☐ Yes ☐ No

8. Breach Readiness

- Do you have a documented breach response plan?

  ☐ Yes ☐ No

- Will your vendors notify you immediately in case of a security incident?

  ☐ Yes ☐ No

- Can you quickly export audit logs if needed?

  ☐ Yes ☐ No

- Do you understand the 60-day breach notification requirement?

  ☐ Yes ☐ No

9. System & Workflow Reality Check

- Are your communication tools integrated (instead of scattered across multiple systems)?

  ☐ Yes ☐ No

- Do staff consistently use approved tools instead of bypassing them?

  ☐ Yes ☐ No

- Do you have full visibility into patient communication history?

  ☐ Yes ☐ No

- Is PHI contained within secure systems (not copied across tools manually)?

  ☐ Yes ☐ No

Your Score

- **40–45 checks** → Low Risk (Well-structured, optimize further)
- **25–39 checks** → Moderate Risk (Gaps that need fixing soon)
- **Below 25** → High Risk (Your communication workflow is exposed)

What Your Score Really Means

- If you scored in the moderate or high-risk range, the issue usually isn't staff behavior.

It's this:

Your current tools weren't built for HIPAA-compliant communication.

Next Step

Instead of patching gaps manually, the faster path is to move to a **unified communication platform** that handles:

- Secure messaging
- Consent management
- Audit logs
- EHR/PMS integration

Book a demo