HOW-TO GUIDE

Secure Email Best Practices

How mental health & behavioral health practices can use email without putting protected health information at risk.

Think of standard email as a postcard

Ordinary email travels in the open and is easy to misdirect — and misdirected email is one of the most common causes of healthcare breaches. The good news: when PHI is properly encrypted, it generally falls under HIPAA's breach "safe harbor," so a lost or intercepted message is far less likely to become a reportable breach. The practices below get you there.

1. Start with a Business Associate Agreement

45 CFR §164.502(e) · §164.308(b)

Before any PHI moves through email, your email provider must be a contracted business associate. No BAA means no PHI — full stop.

- **Sign a BAA with your email provider**
  Microsoft 365 and Google Workspace will sign a BAA — but only on qualifying business plans, not free or personal tiers.
- **Confirm your plan tier is BAA-eligible**
  Verify in writing that your specific subscription covers email; coverage can differ by plan and add-on.
- **Never use consumer email for PHI**
  Personal Gmail, Yahoo, iCloud, or ISP mailboxes cannot be made HIPAA-compliant and have no BAA.

2. Encrypt Everything

45 CFR §164.312(e)(1) · (e)(2)(ii)

Encryption is your single most valuable safeguard. It protects PHI in transit and, when a message is properly encrypted, it's what lets a lost email avoid becoming a reportable breach.

- **Encrypt messages that contain PHI**
  Use your platform's message encryption (e.g., Microsoft Purview / Office Message Encryption) rather than relying on transport security alone.
- **Require TLS for mail in transit**
  Ensure connections are encrypted end-to-end between mail servers so messages aren't readable along the way.
- **Encrypt attachments too**
  PHI in a PDF or spreadsheet needs the same protection as the message body; don't leave it in the clear.

Quick start — encrypting a message in Microsoft 365 / Outlook

1. Open a new message and finish your draft as usual.
2. On the **Options** tab, select **Encrypt** (in new Outlook, use the **Encrypt** button on the toolbar).
3. Choose the protection level — **Encrypt-Only** for most patient communication.
4. Keep PHI out of the subject line, then send. External recipients open it through a secure link or one-time passcode.

3. Practice Minimum Necessary

45 CFR §164.502(b)

Send the least PHI required to get the job done. The information you don't put in an email can't be exposed by one.

- **Keep PHI out of subject lines**
  Subject lines are rarely encrypted and often visible in previews; never include names, diagnoses, or details there.
- **Link to the portal instead of attaching**
  Where possible, send a secure-portal notice rather than emailing records or sensitive documents directly.
- **Trim quoted history before replying**
  Long reply chains accumulate PHI; remove what the new recipient doesn't need to see.

4. Mind the Metadata

45 CFR §164.514(b)

PHI can leak from the parts of an email people forget to check — not just the message body.

- **Watch calendar invites and .ics files**
  An invite that pairs a patient's name with your practice's identity can reveal PHI on its own; keep appointment details generic.
- **Beware "logical deduction" exposure**
  Linking a contact to a behavioral health provider can disclose PHI even with no clinical detail present.
- **Use BCC for group messages**
  When emailing multiple patients, BCC their addresses so recipients can't see one another's identities.

> **The calendar-invite trap**
> Sending a meeting invite from a mental health practice automatically attaches an .ics file and a subject line that may name the patient and the provider together — a quiet PHI disclosure. Strip identifying details from invite subjects and locations.

5. Prevent Misdirected Email

Wrong-recipient sends are a top breach cause

The most common email breach isn't a hacker — it's a message sent to the wrong person. A few habits prevent almost all of them.

Do

- ✓ Verify every recipient address before sending
- ✓ Turn on a send delay / "undo send" window
- ✓ Type addresses fresh for anything sensitive
- ✓ Confirm new contacts by a second channel

Don't

- ✗ Trust autocomplete to pick the right person
- ✗ Use Reply-All on threads containing PHI
- ✗ Forward chains without checking the audience
- ✗ Rush a send at the end of the day

6. Lock Down the Account & Devices

45 CFR §164.312(d) · §164.308(a)(5)

A compromised mailbox exposes every message in it. Protect the account as carefully as the messages.

- **Require multi-factor authentication**
  MFA blocks the vast majority of account-takeover attempts, even when a password is stolen.
- **Use strong, unique passwords**
  Give the mailbox its own long passphrase stored in a password manager — never reused elsewhere.
- **Train staff to spot phishing**
  Most breaches start with a convincing email; teach the team to pause, verify, and report.
- **Secure mobile access and never auto-forward**
  Protect phones with a passcode and remote-wipe, and never forward work email to a personal account.

7. Email Patients the Right Way

45 CFR §164.522(b) · §164.524(c)

Patients have the right to request communication by email — and to receive their records that way. Honor the request while documenting that they understand the trade-offs.

- **Honor reasonable requests for email**
  If a patient asks to be contacted by email, accommodate reasonable requests for confidential communications.
- **Warn of the risk, then document the choice**
  A patient may choose unencrypted email after a light-touch warning; note that they were informed and still preferred it.
- **Offer the secure portal as the default**
  Lead with the safer option, and reserve email for patients who specifically prefer it.

The patient-choice rule
OCR guidance allows a practice to send PHI by unencrypted email to a patient who requests it, as long as the patient was warned of the risk and still prefers email. Capture that warning and preference in writing — it's your documentation if questions ever arise.

8. Make It Routine

45 CFR §164.530(b) · §164.316(b)(2)

Good email hygiene sticks when it's written down, taught, and revisited — not left to memory.

- **Adopt a written email policy**
  Spell out when email may be used for PHI, how to encrypt, and what staff must never send.
- **Train the whole team — and refresh it**
  Include email handling in onboarding and periodic security training.
- **Report a misdirected email right away**
  Treat a wrong-recipient send as a potential incident and run it through your breach-assessment process.
- **Retain and dispose of email as records**
  Emails containing PHI are records — retain them per policy and delete them securely when their time is up.

Want Help Locking Down Your Email?

We'll review your setup, BAAs, and encryption — and make secure email simple for your whole team. Reach out for a free consultation.

CALL **631-388-4274**

EMAIL **support@a1plusai.com**

WEBSITE **a1plusai.com**

SERVING **New York & Long Island**