Healthcare Communications HIPAA Checklist

Did you know the penalties for HIPAA non-compliance?

HIPAA violations can result in **significant financial penalties per incident**, depending on the level of culpability.

HIPAA Civil Penalty Structure (Per Violation)

Culpability Level	Minimum Penalty	Maximum Penalty	Annual Cap
1. No Knowledge	$100	$50,000	$25,000
2. Reasonable Cause	$1,000	$50,000	$100,000
3. Willful Neglect (Timely Corrected)	$10,000	$50,000	$250,000
4. Willful Neglect (Not Timely Corrected)	$50,000	$50,000	$1,500,000

☐ **Business Associate Agreement (BAA) Requirement**

- ☐ A **signed Business Associate Agreement (BAA)** is in place with all phone, fax, VoIP, and cloud communication vendors
- ☐ The BAA clearly defines vendor responsibilities for safeguarding PHI
- ☐ Vendors are prohibited from accessing or using PHI outside of permitted purposes
- ☐ BAAs are reviewed periodically and updated as services change

---

Key Legal Requirements & Best Practices

☐ **Secure Transmission**

- ☐ **Encryption:** Digital and cloud faxes are encrypted in transit (and at rest where applicable)
- ☐ **Secure Systems:** Use encrypted internet fax services or secure physical fax machines in locked areas

- ☐ **Verification:** Fax numbers are verified before sending to prevent misdirection

---

☐ **Administrative Safeguards**

- ☐ **Policies & Training:** Written fax policies exist and staff are trained on proper PHI handling
- ☐ **Access Controls:** Fax machines and software are restricted to authorized users only (no shared passwords)
- ☐ **Audit Trails:** Logs track fax activity (who sent/received, when, and destination)

☐ **Physical Safeguards**

- ☐ **Secure Location:** Physical fax machines are placed in restricted or locked areas
- ☐ **Unattended Faxes:** PHI-containing faxes are never left unattended or publicly visible

---

☐ **Fax Cover Sheets (Required for Physical/Hybrid Faxing)**

- ☐ **Confidentiality Disclaimer:** States the fax contains confidential medical information
- ☐ **No PHI Displayed:** Patient names or identifiers are not shown on the cover sheet
- ☐ **Required Details:** Sender/recipient names, fax numbers, date/time, and "destroy if misdirected" notice

---

HIPAA Phone & Voicemail Compliance Requirements

☐ **Secure Phone Communications**

- ☐ PHI is only discussed with verified patients or authorized representatives
- ☐ Identity verification procedures are used before sharing PHI by phone
- ☐ Staff avoid discussing PHI in public or unsecured areas
- ☐ Minimum necessary information is shared during calls

☐ **Voicemail & Messaging Safeguards**

- ☐ Voicemail messages do not include sensitive PHI unless authorized
- ☐ Generic voicemail greetings are used (no diagnosis or detailed information)
- ☐ Secure voicemail systems require PINs or authentication
- ☐ Voicemail messages containing PHI are retained and deleted according to policy

---

☐ **Call Recording & Monitoring (If Used)**

- ☐ Call recording is disabled unless explicitly required and authorized
- ☐ Patients are notified if calls are recorded
- ☐ Recordings containing PHI are encrypted and access-controlled
- ☐ Retention policies align with HIPAA requirements

☐ **Phone System & Vendor Compliance**

- ☐ Phone and VoIP vendors sign a BAA
- ☐ Calls and voicemails are encrypted where supported
- ☐ System access is role-based (no shared extensions or logins)
- ☐ Audit logs exist for call activity and voicemail access
