

HIPAA Compliance Checklist

Quality Control | US

| | | |
|------------------------|--------------|----------------------------|
| DATE ____/____/____ | ORGANIZATION | PRIVACY / SECURITY OFFICER |
|------------------------|--------------|----------------------------|

PRIVACY RULE

| | OK | NOT OK | | OK | NOT OK |
|--|-----------------------|-----------------------|---|-----------------------|-----------------------|
| Notice of Privacy Practices posted / given | <input type="radio"/> | <input type="radio"/> | Authorization forms for non-TPO disclosures | <input type="radio"/> | <input type="radio"/> |
| Minimum necessary standard applied | <input type="radio"/> | <input type="radio"/> | Accounting of disclosures maintained | <input type="radio"/> | <input type="radio"/> |
| Patient access to records within 30 days | <input type="radio"/> | <input type="radio"/> | | | |
| De-identification procedures documented <input type="checkbox"/> OK <input type="checkbox"/> Not OK <input type="checkbox"/> N/A | | | | | |

SECURITY RULE

| | OK | NOT OK | | OK | NOT OK |
|---|-----------------------|-----------------------|---|-----------------------|-----------------------|
| Security risk analysis conducted (annual) <small>45 CFR 164.308(a)(1) — required</small> | <input type="radio"/> | <input type="radio"/> | Encryption — data at rest and in transit | <input type="radio"/> | <input type="radio"/> |
| Risk management plan implemented | <input type="radio"/> | <input type="radio"/> | Workstation security — screen lock, positioning | <input type="radio"/> | <input type="radio"/> |
| Access controls — unique user IDs | <input type="radio"/> | <input type="radio"/> | Mobile device management policy | <input type="radio"/> | <input type="radio"/> |
| Audit logs enabled and reviewed | <input type="radio"/> | <input type="radio"/> | Backup and disaster recovery tested | <input type="radio"/> | <input type="radio"/> |

BREACH & BUSINESS ASSOCIATES

| | OK | NOT OK | | OK | NOT OK |
|---|-----------------------|-----------------------|--|-----------------------|-----------------------|
| Breach notification policy documented | <input type="radio"/> | <input type="radio"/> | BAAs in place with all business associates | <input type="radio"/> | <input type="radio"/> |
| Breach assessment procedure (4-factor test) | <input type="radio"/> | <input type="radio"/> | BA compliance verified | <input type="radio"/> | <input type="radio"/> |
| 60-day notification timeline understood | <input type="radio"/> | <input type="radio"/> | Breach log maintained | <input type="radio"/> | <input type="radio"/> |

TRAINING & DOCUMENTATION

| | OK | NOT OK | | OK | NOT OK |
|--|-----------------------|-----------------------|--|-----------------------|-----------------------|
| All workforce members trained (annual) | <input type="radio"/> | <input type="radio"/> | Sanction policy in place and enforced | <input type="radio"/> | <input type="radio"/> |
| Training records retained 6 years | <input type="radio"/> | <input type="radio"/> | Complaint procedure documented | <input type="radio"/> | <input type="radio"/> |
| Policies reviewed and updated annually | <input type="radio"/> | <input type="radio"/> | Documentation retained 6 years from creation | <input type="radio"/> | <input type="radio"/> |

ASSESSMENT SUMMARY

Overall HIPAA compliance Compliant Gaps identified Significant gaps

Priority remediation actions

Privacy / Security Officer signature _____

Notes

Go digital with Miratag

Skip the paper — fill checklists faster on the Miratag mobile app. Add photos, videos, notes and signatures. Track compliance in real time. Start free at miratag.com

This template is a general-purpose resource, not tailored to any specific jurisdiction. Each organisation must validate compliance with local regulations.



Scan to view

Go digital with Miratag

Skip the paper — fill checklists faster on the Miratag mobile app. Add photos, videos, notes and signatures. Track compliance in real time. Start free at miratag.com

This template is a general-purpose resource, not tailored to any specific jurisdiction. Each organisation must validate compliance with local regulations.



Scan to view