HIPAA & Privacy Practice Readiness Checklist

HIPAA & PRACTICE OPERATIONS TOOLKIT

- ■ Privacy officer/responsibility assigned
- ■ Notice of Privacy Practices reviewed
- ■ Security risk analysis process established
- ■ Business associate relationships inventoried
- ■ Workforce privacy/security training documented
- ■ Incident-response process established
- ■ Patient rights/request workflow established
- ■ Security responsibility assigned
- ■ Privacy policies current
- ■ Risk-management plan documented
- ■ BAAs reviewed where applicable
- ■ Access controls/user accounts reviewed
- ■ Breach-assessment/reporting workflow established
- ■ Secure disposal process established

Practice _____

Reviewer _____

Priority gaps / owner / due date _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____

Template notice: General educational/operational starting point only. It is not legal, medical, billing, cybersecurity, or regulatory advice and does not guarantee compliance. Customize for the practice, patient population, technology, payer requirements, clinician scope, state/federal law, and current official agency guidance. Obtain qualified legal, privacy/security, billing, and clinical review as applicable.

Workforce Confidentiality & Information Security Acknowledgment

HIPAA & PRACTICE OPERATIONS TOOLKIT

I understand that patient, employee, business, credentialing, financial, and other confidential information may only be accessed, used, or disclosed as authorized for my role and as permitted by applicable law and policy.

- ■ Use unique credentials; do not share passwords
- ■ Protect screens/devices/documents from unauthorized viewing
- ■ Report suspected privacy/security incidents promptly
- ■ Maintain confidentiality after employment/contract ends
- ■ Access only information needed for assigned duties
- ■ Use approved communication/storage systems
- ■ Return or destroy confidential information when directed

Workforce member _____

Role _____

Training completed / date _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____

Template notice: General educational/operational starting point only. It is not legal, medical, billing, cybersecurity, or regulatory advice and does not guarantee compliance. Customize for the practice, patient population, technology, payer requirements, clinician scope, state/federal law, and current official agency guidance. Obtain qualified legal, privacy/security, billing, and clinical review as applicable.

Patient Communication Preferences & Authorization Worksheet

HIPAA & PRACTICE OPERATIONS TOOLKIT

Use this worksheet to document communication preferences. Determine whether a separate HIPAA authorization or other consent is required for the specific disclosure or communication.

- ■ Phone call
- ■ Voicemail
- ■ SMS/text
- ■ Email
- ■ Patient portal
- ■ Mail

Approved phone/email/address _____

Voicemail limitations _____

Persons patient requests involvement with _____

Restrictions / special instructions _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____

Medical Records Release / Authorization Planning Worksheet

HIPAA & PRACTICE OPERATIONS TOOLKIT

This worksheet helps staff collect information needed for an authorization. Use a legally compliant authorization form for the actual disclosure, including any additional requirements for specially protected records.

Patient _____

Recipient / sender _____

Purpose _____

Records / date range _____

Method _____

Expiration/event _____

Specially protected information considerations _____

Identity/authority verified _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____

Privacy / Security Incident Intake Report

HIPAA & PRACTICE OPERATIONS TOOLKIT

Date/time discovered _____

Reporter _____

System/location _____

Individuals/data potentially involved _____

What happened _____

How discovered _____

Immediate containment _____

Devices/accounts/vendors involved _____

Who has been notified internally _____

- ■ Unauthorized access
- ■ Lost/stolen device
- ■ Improper disposal
- ■ Vendor incident
- ■ Misdirected communication
- ■ Malware/phishing
- ■ Credential compromise
- ■ Other

Next assessment step _____

Assigned owner _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____

Template notice: General educational/operational starting point only. It is not legal, medical, billing, cybersecurity, or regulatory advice and does not guarantee compliance. Customize for the practice, patient population, technology, payer requirements, clinician scope, state/federal law, and current official agency guidance. Obtain qualified legal, privacy/security, billing, and clinical review as applicable.

Breach Risk Assessment & Response Worksheet

HIPAA & PRACTICE OPERATIONS TOOLKIT

Use after a suspected impermissible use/disclosure or security incident. This worksheet does not itself determine whether notification is legally required.

Incident reference _____

Nature/extent of information _____

Unauthorized person/entity _____

Whether information was actually acquired/viewed _____

Mitigation completed _____

Risk assessment conclusion / rationale _____

Legal/privacy review _____

Notification decision / deadlines _____

HHS/state/other reporting considerations _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____

Patient Complaint & Grievance Form

HIPAA & PRACTICE OPERATIONS TOOLKIT

Patient / representative _____

Date _____

Contact information _____

Service/provider/location _____

Description of concern _____

Requested resolution _____

Immediate safety issue, if any _____

Staff receiving complaint _____

Investigation / findings _____

Resolution / communication _____

Follow-up / closure _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____

Document Retention & Secure Disposal Planning Checklist

HIPAA & PRACTICE OPERATIONS TOOLKIT

- ■ Federal requirements identified
- ■ Payer/contract requirements identified
- ■ Personnel/business records addressed
- ■ Paper disposal method approved
- ■ Vendor destruction terms reviewed
- ■ State retention requirements identified
- ■ Clinical record retention schedule documented
- ■ Litigation/audit holds addressed
- ■ Electronic media disposal process approved
- ■ Destruction documentation maintained

Record category _____

Retention period/source _____

Responsible owner _____

Disposal method _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____

User Access & Workforce Offboarding Checklist

HIPAA & PRACTICE OPERATIONS TOOLKIT

- ■ Termination/role-change date confirmed
- ■ Email account disabled/modified
- ■ VPN/remote access removed
- ■ Shared secrets/passwords rotated if needed
- ■ Forwarding/delegation reviewed
- ■ Audit/access review considered
- ■ EHR access disabled/modified
- ■ Cloud/storage access removed
- ■ Prescription/eRx access removed
- ■ Devices/keys/badges returned
- ■ Confidentiality reminder provided

Workforce member _____

Role _____

Completed by _____

Exceptions / follow-up _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____

HIPAA Training & Policy Attestation Record

HIPAA & PRACTICE OPERATIONS TOOLKIT

Workforce member _____

Role _____

Training date _____

Training topic/source _____

- ■ Privacy policies reviewed
- ■ Security policies reviewed
- ■ Incident reporting reviewed
- ■ Phishing/social engineering reviewed
- ■ Secure communications reviewed
- ■ Minimum necessary/access expectations reviewed
- ■ Patient rights workflow reviewed
- ■ Questions answered

Additional training required _____

Renewal/review date _____

Workforce / Patient Signature: _____ **Date:** _____

Reviewer / Clinician: _____ **Date:** _____