HIPAA PRIVACY

POLICY & STANDARD OPERATING PROCEDURES

Doctor’s Office / Physician Practice

Practice Name	_____
Policy Number	HIPAA-PRIV-001
Effective Date	September 1, 2026
Review Date	September 1, 2027
Policy Owner	Privacy Officer / Practice Administrator

CONTROLLED DOCUMENT

This manual is a practical HIPAA Privacy template. Customize practice-specific contacts, workflows, state-law requirements, technology controls, and forms before adoption.

Document Control

Field	Current Version	Owner	Review
Policy	1.0	Privacy Officer	Annual
Forms	1.0	Practice Administrator	Annual
Approval	Pending	Practice Leadership	On revision

Table of Contents

1. Purpose and Scope

Purpose

This manual establishes the practice's basic HIPAA Privacy compliance program and operating procedures for protecting Protected Health Information (PHI), responding to patient privacy requests, handling disclosures, managing privacy incidents, and training the workforce.

Scope

This policy applies to physicians, advanced practice clinicians, nurses, medical assistants, front-desk staff, billing personnel, managers, contractors, trainees, volunteers, and other workforce members whose conduct is under the practice's control.

Policy statement

The practice will use and disclose PHI only as permitted or required by applicable law. Workforce members may access PHI only when needed for legitimate treatment, payment, health care operations, or another permitted purpose. Curiosity, convenience, or personal interest is never a valid reason to access a patient record.

2. Roles and Responsibilities

Privacy Officer

The Privacy Officer oversees the HIPAA Privacy Program, maintains privacy policies, coordinates training, receives complaints, investigates privacy incidents, coordinates breach assessments, maintains required documentation, and reports significant issues to practice leadership.

Practice Administrator

The Practice Administrator supports implementation, staffing, resources, disciplinary processes, vendor management, and operational enforcement.

Workforce members

Every workforce member is responsible for protecting PHI, following approved procedures, completing required training, using only approved systems, securing records, and promptly reporting suspected privacy incidents.

Clinical leadership

Clinical leadership supports appropriate access to records, patient communications, release-of-information decisions, and corrective action when privacy risks are identified.

3. Patient Privacy and Minimum Necessary

Front desk and waiting room

Use reasonable safeguards to prevent unnecessary overhearing or viewing of PHI. Avoid detailed discussions of diagnoses in public areas, position monitors away from public view, secure paper records, and use patient identifiers discreetly.

Telephone

Verify identity before providing PHI when appropriate. Do not provide detailed information to an unidentified caller. Follow the practice's approved verification process.

Voicemail

Use limited information unless the patient has specifically authorized a more detailed message. A typical message may identify the practice, patient, and callback number without stating a diagnosis or test result.

Minimum necessary

When the minimum-necessary standard applies, limit access, use, or disclosure to the amount reasonably necessary for the intended purpose. Note that HIPAA contains exceptions to the minimum-necessary standard.

Incidental disclosures

The practice will use reasonable safeguards to minimize incidental disclosures. Examples include closing doors, lowering voices, using privacy screens, and avoiding unnecessary conversations in hallways.

Operating Standard

Step	Responsible	Required Action
1	All staff	Use reasonable safeguards in public areas.
2	All staff	Verify identity before appropriate disclosures.
3	All staff	Use only the PHI needed for the task.
4	Supervisor	Escalate questionable disclosures.

4. Electronic Communications and Social Media

Email

Use practice-approved systems. Verify recipients before sending PHI, minimize the information included, and use secure/encrypted methods when required by the practice's technology configuration or risk assessment. Never forward PHI to personal email accounts.

Texting and messaging

Do not use personal phones or consumer messaging applications for PHI unless the practice has specifically approved the technology and implemented appropriate safeguards.

Photography and video

Do not photograph patients, charts, screens, or other PHI with personal devices unless specifically authorized and consistent with practice procedures.

Social media

Do not post patient names, photographs, diagnoses, treatment details, or stories that could reasonably identify a patient without an appropriate authorization. Removing a name does not necessarily make a post non-identifiable.

5. Medical Records and Patient Rights

Access to records

Patients generally have a HIPAA right of access to PHI in designated record sets, subject to limited exceptions. Requests must be routed through the practice's designated records process and completed within applicable federal and state requirements.

Amendment requests

Patients may request an amendment to PHI. Staff must not alter or delete a record simply because a patient requests a change. Refer requests to the Privacy Officer or Medical Records Officer.

Confidential communications

Patients may request communications by alternative means or at alternative locations when applicable. Staff should route these requests to the designated privacy/records contact.

Restrictions

Patients may request restrictions on certain uses and disclosures. Requests must be evaluated under HIPAA and applicable practice/state procedures.

Accounting of disclosures

When required, the practice will maintain appropriate documentation to respond to accounting requests. Disclosures for treatment, payment, and health care operations are generally treated differently under HIPAA's accounting requirements.

Operating Standard

Step	Responsible	Required Action
1	Records staff	Log and verify the request.
2	Records staff	Identify the designated record set requested.
3	Privacy Officer	Resolve exceptions or unusual requests.
4	Records staff	Document completion and delivery.

6. Notice of Privacy Practices and Authorizations

Notice of Privacy Practices

The practice will maintain a current Notice of Privacy Practices (NPP), provide it as required, make it available upon request, and prominently post it on any applicable practice website. The NPP must accurately describe the practice's uses and disclosures, patient rights, complaint process, and legal duties.

Acknowledgment

The practice may request a written acknowledgment that the patient received the NPP. A patient's refusal to sign the acknowledgment does not, by itself, prevent the practice from using or disclosing PHI as permitted by HIPAA.

Authorizations

When HIPAA requires an authorization, staff must obtain a valid authorization before making the disclosure. Unusual or questionable requests must be referred to the Privacy Officer.

State law

Where applicable, the practice will follow state privacy laws that provide greater protection than HIPAA. The Privacy Officer should obtain legal/compliance guidance when state-law requirements are unclear.

7. Business Associates and Vendors

Identification

The practice will identify vendors and service providers that meet the HIPAA definition of Business Associate.

Business Associate Agreements

Where required, the practice will execute a Business Associate Agreement (BAA) before permitting a Business Associate to receive or access PHI.

Vendor review

The practice should maintain a current list of Business Associates, review agreements periodically, and address material changes in services or technology.

Examples

Depending on the services provided, Business Associates may include billing companies, certain IT/cloud providers, medical-record vendors, practice-management companies, consultants, and other organizations that handle PHI on the practice's behalf.

8. Privacy Incident and Breach Response SOP

Report immediately

Workforce members must promptly report suspected unauthorized access, use, disclosure, loss, or improper handling of PHI to the Privacy Officer. Do not conceal or delete evidence.

Examples

Examples include sending records to the wrong patient, emailing PHI to the wrong recipient, losing a chart, leaving a chart in a public area, accessing a record without a legitimate work reason, or losing a device containing PHI.

Initial response

The Privacy Officer should secure the information, preserve relevant evidence, identify affected systems and individuals, determine what PHI was involved, and document the date and discovery circumstances.

Breach assessment

For an impermissible use or disclosure of unsecured PHI, the practice will evaluate whether an exception applies and, when required, conduct and document a breach risk assessment. The assessment should consider the nature and extent of PHI, the unauthorized recipient/person, whether PHI was actually acquired or viewed, and mitigation.

Notification

If notification is required, the practice will follow HIPAA and applicable state requirements. Federal HIPAA individual notices generally must be provided without unreasonable delay and no later than 60 days after discovery of a breach of unsecured PHI. The Secretary of HHS must also be notified; breaches affecting 500 or more individuals have a 60-day federal reporting deadline, while breaches affecting fewer than 500 may generally be reported annually.

Documentation

Maintain documentation supporting the determination that notification was or was not required, including the risk assessment and any applicable exception.

Operating Standard

Step	Responsible	Required Action
1	Reporter	Immediately notify Privacy Officer.
2	Privacy Officer	Contain, preserve evidence, identify PHI.
3	Privacy Officer	Conduct/document breach assessment as required.
4	Leadership	Approve notifications and corrective action.

9. Workforce Training, Sanctions, and Complaints

Training

Provide HIPAA Privacy training at onboarding and periodically thereafter, and when material policy or regulatory changes occur. Training should be role-based and documented.

Sanctions

The practice will apply appropriate sanctions for workforce violations, consistent with policy and applicable law. Factors may include intent, severity, scope, prior history, cooperation, and whether the employee promptly reported the issue.

Patient complaints

Patients may submit privacy complaints to the practice without fear of retaliation. Complaints must be routed to the Privacy Officer, investigated, documented, and resolved as appropriate.

Non-retaliation

The practice prohibits retaliation against a patient or workforce member for making a good-faith privacy complaint or reporting a suspected privacy violation.

10. Documentation and Annual Review

Documentation

Maintain HIPAA-required documentation, including policies and procedures, training records, complaints, investigations, breach assessments, notifications, Business Associate Agreements, and other required records.

Retention

HIPAA documentation generally must be retained for at least six years from creation or the date it was last in effect, whichever is later, unless a longer period is required by state law, contract, litigation hold, or another applicable requirement.

Annual review

At least annually, review privacy policies, incidents, complaints, EHR access controls, training, Business Associate Agreements, patient-request workflows, the NPP, and changes in technology and law.

Approval

Material changes should be reviewed and approved by practice leadership and, when appropriate, qualified legal/compliance counsel.

Appendix A — Employee HIPAA Privacy Acknowledgment

I acknowledge that I have received, reviewed, and understand the practice's HIPAA Privacy Policy & SOP Manual.

I understand that I may access, use, or disclose PHI only for legitimate work-related purposes and as permitted by law and practice policy.

I understand that suspected privacy incidents must be reported promptly and that violations may result in disciplinary action.

Employee Name: _____

Signature: _____

Date: _____ Supervisor: _____

Appendix B — HIPAA Privacy Incident Report

Date/time discovered: _____

Reported by: _____

Date/time reported: _____

Patient(s) potentially affected: _____

Description of incident: _____

_____

Type of PHI involved: _____

How was the incident discovered? _____

Immediate containment/mitigation steps: _____

_____

Recipient/person who accessed or received PHI (if known): _____

Privacy Officer review date: _____

Risk assessment required? ■ Yes ■ No ■ Pending

Notification required? ■ Yes ■ No ■ Pending

Corrective action: _____

Privacy Officer signature/date: _____

Appendix C — Patient Medical Record Request Intake Checklist

■ Verify patient identity / personal representative authority as appropriate

■ Date request received: _____

■ Requested records / designated record set identified

■ Requested format: ■ Paper ■ Electronic ■ Other: _____

■ Delivery method and destination verified

■ Any applicable state-law requirements identified

■ Request routed to records/privacy contact

■ Response date: _____

■ Any denial/limitation reviewed by authorized staff

■ Copy of request and response retained according to practice policy

Appendix D — Annual HIPAA Privacy Compliance Checklist

■ Current Privacy Policy & SOP reviewed

■ Notice of Privacy Practices reviewed and current

■ Workforce HIPAA training completed/documented

■ Privacy complaints reviewed

■ Privacy incidents/breach assessments reviewed

■ EHR access and user accounts reviewed

■ Business Associate list and BAAs reviewed

■ Medical-record request process reviewed

■ Authorization forms reviewed

■ Email/texting workflows reviewed

■ Secure disposal procedures reviewed

■ State privacy-law changes reviewed

■ Corrective actions tracked to completion

Reviewed by: _____ Date: _____

References and Regulatory Notes

This template was prepared using current HHS Office for Civil Rights materials reviewed during preparation. Verify current requirements before adoption and whenever this policy is revised.

HHS Office for Civil Rights — Summary of the HIPAA Privacy Rule: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

HHS Office for Civil Rights — Breach Notification Rule: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

HHS Office for Civil Rights — Notice of Privacy Practices:
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/privacy-practices-for-protected-health-information/index.html

HHS Office for Civil Rights — Model Notice of Privacy Practices (February 2026):
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html

HHS Office for Civil Rights — Summary of the HIPAA Security Rule (reviewed August 7, 2026):
https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Practice-Specific Completion Items

- ■ Insert practice legal name and address.
- ■ Name the Privacy Officer and backup contact.
- ■ Add practice-specific medical-record request and authorization forms.
- ■ Identify approved email, messaging, EHR, cloud, and document-destruction systems.
- ■ Complete and maintain the Business Associate inventory.
- ■ Confirm state-specific privacy, medical-record, minor-consent, and breach-notification requirements.
- ■ Review the current Notice of Privacy Practices before implementation.
- ■ Coordinate this Privacy manual with the separate HIPAA Security Rule / Security Risk Assessment program.