

OCR-Ready Governance Evidence File

Sample Phase 1 Governance Pack for an Independent Medical Practice

Purpose. This sample evidence file is designed to help an independent medical or dental practice organize the governance evidence supporting its HIPAA Security Rule compliance program. Replace all bracketed fields with practice-specific information and retain supporting records.

Important. This is a model template, not legal advice and not a substitute for a practice-specific Security Risk Analysis (SRA). Policies and assignments should reflect the practice's actual operations.

1. Governance Evidence Index

Evidence ID	Document / Record	Owner	Status
GOV-01	Security Official Designation	Practice Administrator	☐ Current
GOV-02	HIPAA Security Responsibilities Matrix	Security Official	☐ Current
GOV-03	HIPAA Security Policy Approval Record	Practice Leadership	☐ Current
GOV-04	Workforce Security & Training Record	Compliance Coordinator	☐ Current
GOV-05	Business Associate Agreement Register	Practice Administrator	☐ Current
GOV-06	Incident Response Responsibility & Escalation Record	Security Official	☐ Current
GOV-07	Annual Governance Review Record	Practice Leadership	☐ Current

2. Practice Profile

Practice legal name	[Sample Medical Practice, PLLC]
Practice type	[Primary care/specialty / dental/behavioral health]
Practice address	[Address]
Practice administrator	[Name / title]
Managing physician / owner	[Name/title]
HIPAA Security Official	[Name/title]
Privacy Official	[Name/title]
IT provider / MSP	[Vendor/contact]
EHR / practice management system	[System/vendor]
Effective date of this governance file	[MM/DD/YYYY]
Last governance review	[MM/DD/YYYY]
Next scheduled review	[MM/DD/YYYY]

3. GOV-01 — Security Official Designation

The practice designates the following individual as responsible for the development and implementation of its security policies and procedures under the HIPAA Security Rule.

Name	[Jane Smith]
Title	[Practice Administrator / Compliance Coordinator]
Effective date	[MM/DD/YYYY]
Authority	Responsible for coordinating Security Rule compliance, risk-management activities, remediation tracking, workforce coordination and security documentation.
Backup / alternate	[Name / title]

Acknowledgment: I understand the responsibilities assigned to me and will escalate material security risks to practice leadership.

Signature: _____ Date: _____

Practice leadership approval: _____ Date: _____

4. GOV-02 — HIPAA Security Responsibilities Matrix

Function	Responsible Role	Backup	Review Frequency	Evidence
Security Rule administration	Security Official	[Backup]	Annual + as needed	GOV-01; review record
Security Risk Analysis	Security Official + IT	[Backup]	At least annually / when environment changes	SRA + remediation plan
Access management	IT / EHR Administrator	[Backup]	Monthly / on personnel change	Access review
Workforce security	Practice Administrator	[Backup]	Onboarding / termination	Training & termination records
Business associates	Practice Administrator	[Backup]	At onboarding + contract review	BAA register
Incident response	Security Official	[Backup]	After incident / annual test	Incident log / exercise
Backup & recovery	IT Provider	[Backup]	Periodic testing	Backup / restore evidence
Policy review	Practice Leadership	[Backup]	Annual	Approval record

5. GOV-03 — Security Policy Approval Record

Practice leadership confirms that the practice has reviewed and approved its current HIPAA Security Rule policies and procedures.

Policy / Procedure	Version	Effective Date	Approved By
HIPAA Security Policy	1.0	[Date]	[Name / title]
Access Control Procedure	1.0	[Date]	[Name / title]
Incident Response Procedure	1.0	[Date]	[Name / title]
Backup & Recovery Procedure	1.0	[Date]	[Name / title]
Workforce Security Procedure	1.0	[Date]	[Name / title]

Approval signature: _____ Date: _____

Next scheduled policy review: _____

6. GOV-04 — Workforce Security & Training Record

The practice maintains evidence that members of the workforce receive security awareness training appropriate to their responsibilities and that access is managed when workforce members join, change roles or leave.

Employee / Role	Start / Change Date	Training Date	Access Reviewed	Record Location
[Name / role]	[Date]	[Date]	☐ Yes ☐ N/A	[Folder / system]
[Name / role]	[Date]	[Date]	☐ Yes ☐ N/A	[Folder / system]
[Name / role]	[Date]	[Date]	☐ Yes ☐ N/A	[Folder / system]
[Name / role]	[Date]	[Date]	☐ Yes ☐ N/A	[Folder / system]
[Name / role]	[Date]	[Date]	☐ Yes ☐ N/A	[Folder / system]

Minimum evidence to retain: training completion, security awareness content/version, acknowledgment where used, and access/termination records.

7. GOV-05 — Business Associate Agreement Register

Use this register to identify vendors that may create, receive, maintain or transmit PHI and to track the status of required business associate arrangements.

Vendor	Service	PHI Access?	BAA Status	Last Review
EHR Vendor	Electronic health record	☐ Yes	☐ Executed	[Date]

Cloud Email Provider	Email / collaboration	☐ Yes	☐ Executed	[Date]
Billing Company	Revenue cycle management	☐ Yes	☐ Executed	[Date]
IT / MSP	IT support / remote administration	☐ Yes	☐ Executed	[Date]
Backup Provider	Data backup / recovery	☐ Yes	☐ Executed	[Date]

8. GOV-06 — Incident Response Responsibility & Escalation

The practice maintains a documented process for escalating suspected security incidents, including unauthorized access, malware/ransomware, lost devices, credential compromise and material system outages.

Role	Responsibility	Contact / Backup
First reporter	Immediately report suspected incident	[Method / contact]
Security Official	Coordinate containment and documentation	[Name / phone]
IT / MSP	Technical investigation and containment	[Vendor / phone]
Privacy Official	Assess privacy / breach implications	[Name / phone]
Practice Leadership	Approve material response decisions	[Name / phone]
Legal counsel	Legal assessment when engaged	[Firm / contact]

Incident reporting channel: [email / phone / ticketing system]

Emergency escalation: [24/7 contact, if applicable]

9. GOV-07 — Annual Governance Review

At least annually, and following material changes to the practice environment, leadership should review the governance program and document the result.

- ☐ Security official designation remains current.
- ☐ Security responsibilities remain assigned.
- ☐ Current Security Risk Analysis is on file.
- ☐ Material risks have assigned owners and remediation status.
- ☐ Policies and procedures reflect current operations.
- ☐ Workforce training records are current.
- ☐ Business associate register has been reviewed.
- ☐ Incident-response contacts are current.
- ☐ Material changes in systems, vendors, locations or workforce have been assessed.
- ☐ Governance evidence is retained in the designated compliance repository.

Review outcome: ☐ No material changes ☐ Remediation required ☐ SRA update required ☐ Leadership escalation required

Reviewer: _____ Date: _____

Leadership approval: _____ Date: _____

10. Evidence Repository Structure

Recommended folder structure:

- 01_Governance
- 02_Security_Risk_Analysis
- 03_Risk_Register_and_Remediation
- 04_Policies_and_Procedures
- 05_Asset_and_ePHI_Inventory
- 06_Access_Controls
- 07_Training
- 08_Vendors_and_BAAs
- 09_Incident_Response
- 10_Backup_and_Recovery
- 11_Audit_and_Monitoring
- 12_Testing_and_Reviews

Access to the repository should itself be restricted and appropriate for the sensitivity of the records it contains.

11. OCR Readiness Check

Question	Yes / No	Evidence Reference
Can the practice identify its Security Official?	☐ Yes ☐ No	[GOV-__ / file path]
Can leadership show who owns each major Security Rule responsibility?	☐ Yes ☐ No	[GOV-__ / file path]
Are current policies approved and dated?	☐ Yes ☐ No	[GOV-__ / file path]
Can the practice produce workforce security/training evidence?	☐ Yes ☐ No	[GOV-__ / file path]
Can the practice identify business associates and BAA status?	☐ Yes ☐ No	[GOV-__ / file path]
Is there a documented incident escalation process?	☐ Yes ☐ No	[GOV-__ / file path]
Is the current SRA readily accessible?	☐ Yes ☐ No	[GOV-__ / file path]
Can the practice demonstrate that governance documents reflect actual operations?	☐ Yes ☐ No	[GOV-__ / file path]

12. Document Control

Document owner	[Security Official]
Version	1.0
Effective date	[MM/DD/YYYY]
Review frequency	At least annually and upon material change
Approved by	[Practice leadership]
Retention	Retain in accordance with applicable HIPAA documentation requirements and the practice's records-retention policy.

SAMPLE TEMPLATE — Replace bracketed fields and attach supporting evidence before relying on this file.