

HIPAA Compliance Review Checklist

Use this administrative checklist to organize periodic privacy, security and breach-response review activities.

Organization _____	Review Period _____
Reviewer _____	Next Review _____

Governance & Documentation

- ☐ Privacy and security responsibility is assigned.
- ☐ Policies and procedures are reviewed and updated as needed.
- ☐ Workforce training is current and documented.
- ☐ Business associate inventory and agreements are maintained.

Privacy

- ☐ Uses and disclosures are limited to permitted purposes.
- ☐ Minimum necessary practices are addressed.
- ☐ Patient rights requests have defined workflows.
- ☐ Notice of Privacy Practices is current and available as required.

Security

- ☐ Security risk analysis is current.
- ☐ Access controls and unique user accounts are managed.
- ☐ Workstation, device and media controls are documented.
- ☐ Backup, recovery and contingency procedures are tested.
- ☐ Technical safeguards and audit / logging capabilities are reviewed.

Incident & Breach Response

- ☐ Workforce knows how to report suspected incidents.
- ☐ Incident investigation and risk assessment workflow is documented.
- ☐ Breach notification responsibilities and timelines are understood.
- ☐ Corrective actions are tracked to completion.

This checklist is a general administrative resource, not legal advice or a certification of HIPAA compliance. Use current HHS guidance and qualified privacy/security counsel for organization-specific obligations.