Sage Health Privacy
PRIVACY EXPERTISE FOR A HEALTHIER TOMORROW

HIPAA PRIVACY RULE COMPLIANCE & RISK ASSESSMENT

Comprehensive Internal Assessment Tool for Healthcare Providers

Organization Name: _____ Date of Assessment: _____

1. Notice of Privacy Practices (NPP) & Patient Communication

Status	Assessment Area	Compliance Criteria
[ ] Yes [ ] No	**Up-to-Date NPP:**	Does the organization have a written Notice of Privacy Practices that accurately describes how it handles and protects Protected Health Information (PHI)?
[ ] Yes [ ] No	**NPP Distribution:**	Is the NPP prominently displayed in physical waiting areas and posted directly on the public website?
[ ] Yes [ ] No	**Good Faith Acknowledgment:**	Does the organization make a documented, good-faith effort to obtain a signed written acknowledgment of receipt from patients on their first day of service?
[ ] Yes [ ] No	**Alternative Communications:**	Are reasonable requests to receive health communications by alternative methods or at alternative locations accommodated (e.g., calling a cell phone instead of a home phone)?

2. Patient Rights & Controls Over PHI

Status	Assessment Area	Compliance Criteria
[ ] Yes [ ] No	**Right to Access & Copy:**	Is there a functional workflow to allow patients to inspect and obtain copies of their health records within the federal 30-day requirement?
[ ] Yes [ ] No	**Right to Amend:**	Is there a clear operational policy for processing formal patient requests to amend incorrect or incomplete data in their medical records?
[ ] Yes [ ] No	**Right to Restrict Disclosures:**	Are procedures in place to restrict disclosures of PHI to insurance plans if the patient paid out-of-pocket in full and requested the restriction?
[ ] Yes [ ] No	**Accounting of Disclosures Log:**	Does the organization maintain a baseline internal log to track non-routine or impermissible external disclosures of PHI for patient accounting requests?

3. Uses and Disclosures of PHI

Status	Assessment Area	Compliance Criteria
[ ] Yes [ ] No	**Minimum Necessary Standard:**	Are internal data flows and user access privileges limited so staff only access the minimum amount of PHI required to perform their jobs?

Sage Health Privacy
PRIVACY EXPERTISE FOR A HEALTHIER TOMORROW

[ ] Yes [ ] No	**Incidental Disclosure Mitigation:**	Are administrative safeguards in place to stop accidental visual or audible sharing of PHI (e.g., computer privacy screens, speaking in lowered voices)?
[ ] Yes [ ] No	**Valid Patient Authorizations:**	Does the organization obtain a specific, signed HIPAA Authorization form before sharing PHI for marketing, fundraising, or any purpose outside of Treatment, Payment, or Operations (TPO)?
[ ] Yes [ ] No	**Opportunity to Object:**	Is there a clear clinical protocol to verify a patient's verbal agreement or give them an opportunity to object before discussing health details with family or friends?

4. Privacy Administration & Privacy Safeguards

Status	Assessment Area	Compliance Criteria
[ ] Yes [ ] No	**Designated Privacy Officer:**	Has the organization formally designated and empowered a Privacy Officer to monitor compliance and manage patient privacy complaints?
[ ] Yes [ ] No	**State Privacy Laws**	Has the organization assessed additional state specific privacy laws and implemented related policies and procedures?
[ ] Yes [ ] No	**Privacy Training:**	Have all employees, contractors, volunteers, and new hires received documented training on the organization's unique HIPAA Privacy policies to include any state privacy training?
[ ] Yes [ ] No	**Business Associate Agreements (BAA):**	Are signed BAAs securely filed for every third-party vendor that creates, receives, maintains, or transmits PHI on your behalf (e.g., AI tools, cloud services, billing companies, shredding services)?
[ ] Yes [ ] No	**Internal Complaint Process:**	Is there a clear, non-retaliatory process for patients and staff members to submit formal internal privacy complaints?

5. Summary & Action Plan

Total Compliant Items: _____ / 16

High-Priority Vulnerabilities Identified:

_____

Corrective Remediation Plan:

Corrective Action Required	Target Date	Owner