HIPAA Compliance Checklist

HIPAA Compliance Checklist

Determine Your Status

Assess if your organization is a Covered Entity.
Determine if your organization acts as a Business Associate.
Understand obligations under HIPAA even if not a Covered Entity or Business Associate.

Assign Responsibility

Designate a HIPAA Compliance Officer or a HIPAA Privacy Officer and a HIPAA Security Officer.

Understand and Implement HIPAA Rules

Familiarize yourself with the Privacy, Security, Omnibus, and Breach Notification Rules.
Privacy Rule: Implement safeguards for all Protected Health Information (PHI).
Security Rule: Ensure administrative, physical, and technical safeguards are in place for electronic PHI (ePHI).
Breach Notification Rule: Establish procedures for notifying individuals, HHS, and sometimes the media of breaches.
Ensure compliance with the Omnibus Rule, extending requirements to Business Associates.

Conduct a Risk Analysis

Identify and analyze potential risks to ePHI.
Make risk analysis an ongoing process, adapting to changes.

Train Your Staff

Train all workforce members on PHI policies and procedures.

Develop and Implement Policies and Procedures

Create written policies and procedures tailored to your practices and HIPAA requirements.
Regularly review and update policies and procedures.

Maintain Documentation

Keep detailed documentation of HIPAA compliance efforts.

Secure Patient Data

Implement safeguards to protect PHI.
Maintain and update IT infrastructure to secure PHI.

Address Gaps and Violations

Develop corrective action plans for risks or violations.
Record incidents and remediation efforts.

Reporting and Breach Notification

Prepare to report security incidents in compliance with the Breach Notification Rule.

www.nextdlp.com