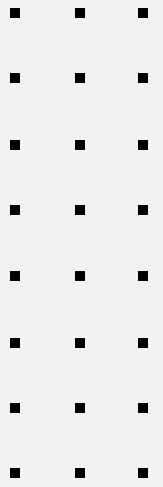


HIPAA Compliance Checklist



1. Form a Compliance Team or Function

- Create a dedicated compliance team that includes stakeholders from across the organization
- Ensure your compliance team reads and understands the HIPAA rules—Privacy, Security, and Breach Notification
- Determine whether your organization is a covered entity or business associate

2. Conduct a HIPAA Risk Assessment

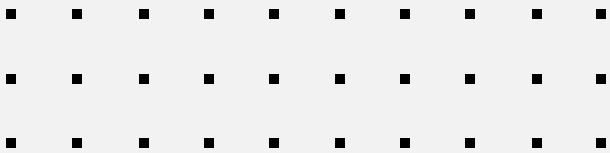
- Determine what PHI you have access to
- Review your current security policies and procedures
- Identify vulnerabilities and the likelihood of potential threats
- Prioritize risks based on their impacts and probabilities
- Document your findings

3. Develop a Compliance Plan

- Build a compliance plan by aligning your prioritized risks with the administrative, physical, and technical safeguards that the HIPAA Security Rule requires

- **Administrative safeguards** include security risk management processes, access controls, training, and incident response planning.
- **Physical safeguards** include measures that control physical access to your network infrastructure and endpoints.
- **Technical safeguards** include the hardware and software that control and monitor PHI access as well as protect PHI at rest and in transit.





4. Implement Your Plans Internally

- Establish HIPAA compliance safeguards
- Gain executive leadership buy-in to aid with adoption of new policies and procedures

5. Determine Which Vendors Must Sign a Business Associate Agreement

- Identify business associates among your vendors
- Create and share business associate agreements with all business associates
- Conduct periodic third-party risk assessments to ensure business associates align with your compliance policies

6. Report Data Breaches Immediately

- Ensure incident response plans align with the HIPAA Breach Notification Rule

When a breach occurs, ensure you:

- Directly contact all patients affected by the breach via written or emailed notifications within 60 days of the breach's discovery
 - If direct contact is not possible, you may need to post notices on your website or in local newspapers
- Ensure that notices to patients are written in plain language
- Report all breaches of unsecured PHI to the Department of Health and Human Services (HHS)
- Report large breaches affecting more than 500 people within 60 days; an annual report to the HHS can summarize smaller breaches
- Notify media organizations of large breaches