HIPAA Compliance Checklist

Keeping up with compliance can be intimidating, but Exym is here to make your job a little easier. Use this printable checklist to ensure your systems are buttoned up to avoid breaches, HIPAA violations, and other privacy and safety infractions.

Required Assessments and Audits

☐ Security Risk Assessment
☐ Privacy Standards Audit
☐ HITECH Subtitle D Privacy Audit
☐ Security Standards Audit
☐ Asset and Device Audit
☐ Physical Site Audit

Remediation Plans

☐ Created remediation plans in writing to address deficiencies found in the above audits

☐ Documented remediation plans are kept for 6 years in case of an audit

☐ Review and update remediation plans every 6 to 12 months

Staff Training and Documentation

☐ At least one staff member is designated as the HIPAA Compliance Officer

☐ Annual HIPAA training for all staff members with documentation of completion

☐ Tailored policies and procedures are documented and easily accessed by all staff members to ensure knowledge and accountability

☐ Documentation of a defined process for incidents and breaches

HIPAA Compliance Checklist

Required Assessments and Audits

☐ Set and implement company-wide password protocol, to ensure employees are:

- ☐ Creating a new password for every site, program, device, etc.
- ☐ Passwords are at least eight characters with a combination of upper and lower case letters, at least one number, and special character
- ☐ Passwords are not stored on a piece of paper, Google or Word doc, or any other insecure document. We recommend using a password manager, which is often very affordable and intuitive
- ☐ Passwords are changed quarterly

☐ Anti-virus software is set up and regularly updated

☐ Employees complete anti-phishing and hacking training

☐ Client data is securely backed up and can be accessed in the event of an emergency or natural disaster

☐ User permissions are granted on a need-to-know basis so not every employee has access to unnecessary information

☐ Protected health information is encrypted at rest and in transmission

☐ Documentation of all your vendors and Business Associates with access or potential access to personal health information

☐ Business Associate Agreements are in place with all vendors and they have strict security measures and training

Exym EHR software's built-in compliance assistance and our customized implementation sets our customers up for success, allowing them to focus on what they do best: caring for clients.