The HIPAA compliant email checklist

Ensure your organization's email is HIPAA compliant with this simple checklist

1. Determine HIPAA applicability and scope

☐ Are you a covered entity or a business associate?

2. Select an email service provider

☐ Choose between Google Workspace and Microsoft 365

☐ Establish a business associate agreement with Google Workspace and Microsoft 365

☐ Connect Paubox to your chosen email provider to encrypt all emails by default

☐ Set up DKIM and SPF records to ensure secure delivery of emails

☐ Send a test email to verify encryption

3. Develop access control policies

☐ Define who can access what types of ePHI

☐ Set guidelines for password complexity

☐ Activate two-factor authentication

PAUBOX

4. Establish email usage policies

- [ ] Develop guidelines on how ePHI should be handled and shared via email

- [ ] Incorporate data retention and deletion policies to establish how long emails containing PHI should be kept

5. Document compliance measures

- [ ] Keep detailed records of all the compliance measures, decisions, and policies implemented

6. Train staff regularly

- [ ] Train staff on HIPAA rules and secure email practices

- [ ] Educate staff on internal email policies

7. Conduct regular risk assessments

- [ ] Regularly review and update security measures and policies

PAUBOX

8. Implement an incident response plan

- [ ] Create a plan for responding to and reporting any security incidents
- [ ] Train staff on breach response protocols

9. Review and Update Policies

- [ ] Schedule regular policy reviews to ensure email policies and practices stay current with HIPAA regulations

10. Document Compliance Measures

- [ ] Maintain a dedicated folder for all HIPAA related documents
- [ ] Log dates and content of training sessions, policy updates, and risk assessments

11. Inbound email security

- [ ] Implement inbound email security, including ExecProtect and Geofencing
- [ ] Set up notifications when a display name spoofing attempt is caught by ExecProtect
- [ ] Train staff to recognize phishing emails

PAUBOX