HIPAA Compliance Checklist

Checklist · 27 items · 8 sections

A comprehensive HIPAA compliance checklist covering the Security Rule, Privacy Rule, and Breach Notification Rule: for healthcare providers, health plans, and business associates.

Open the editable version online:
https://genechecklist.com/checklist/hipaa-compliance-checklist

GOVERNANCE

- [ ] Designate a HIPAA Privacy Officer (required for all covered entities)
  HIGH
- [ ] Designate a HIPAA Security Officer (required for all covered entities)
  HIGH
- [ ] Conduct and document an annual Risk Analysis: identify all PHI and vulnerabilities
  HIGH
  Risk Analysis is required by the Security Rule and is the most commonly cited compliance gap
- [ ] Create and maintain Risk Management Plan with mitigation strategies
  HIGH
- [ ] Develop and maintain written HIPAA policies and procedures
  HIGH

TRAINING

- [ ] Train all workforce members on HIPAA policies (required at hire and annually)
  HIGH
- [ ] Document all training with attendance records and completion dates
  HIGH

PRIVACY RULE

- [ ] Publish Notice of Privacy Practices (NPP) and provide to patients
  HIGH
- [ ] Obtain patient authorization before using PHI for marketing or sale
  HIGH
- [ ] Implement minimum necessary standard: share only the PHI needed for each purpose
  HIGH
- [ ] Process patient requests to access, amend, and restrict their PHI within required timeframes
  HIGH

Access requests: 30 days (extendable to 60). Amendment requests: 60 days

- [ ] Maintain an Accounting of Disclosures log for disclosures not for treatment/payment/operations

HIGH

BUSINESS ASSOCIATES

- [ ] Execute Business Associate Agreements (BAA) with all vendors who access PHI

HIGH

This includes cloud storage providers, billing companies, EHR vendors, IT support firms

- [ ] Maintain list of all Business Associates and keep BAAs current

HIGH

SECURITY RULE: TECHNICAL

- [ ] Encrypt all PHI at rest and in transit (addressable: required if reasonable)

HIGH

- [ ] Implement unique user IDs and access controls: no shared passwords

HIGH

- [ ] Enable automatic log-off for systems containing ePHI

HIGH

- [ ] Maintain audit logs of who accessed, modified, or deleted ePHI

HIGH

- [ ] Implement multi-factor authentication for access to ePHI systems

HIGH

SECURITY RULE: PHYSICAL

- [ ] Implement physical access controls to areas where ePHI is stored

HIGH

- [ ] Establish policies for workstation use and screen positioning in public areas

HIGH

- [ ] Establish media disposal procedures: shred paper PHI, wipe or destroy drives

HIGH

SECURITY RULE: ADMINISTRATIVE

- [ ] Maintain contingency plan: data backup, disaster recovery, emergency access procedures

HIGH

BREACH NOTIFICATION

- [ ] Have documented breach response procedure in place before a breach occurs

HIGH

- [ ] Notify affected individuals within 60 days of discovering a PHI breach

HIGH

- [ ] Report breaches of 500+ individuals to HHS and local media without unreasonable delay

HIGH

- [ ] Report breaches under 500 individuals to HHS annually (within 60 days of year end)

  HIGH