# HIPAA Compliance Checklist



The following are identified by HHS OCR as elements of an effective compliance program. This checklist is available for you to self-evaluate your organization.

## Have you conducted the following required annual audits and assessments?

- ☐ Cybersecurity Risk Assessment
- ☐ Privacy Standards Audit (Not required for BAs)
- ☐ HITECH Subtitle D Privacy Audit
- ☐ Security Standards Audit
- ☐ Asset and Device Audit
- ☐ Physical Site Audit

## Have you identified all gaps uncovered in the audits above?

- ☐ Have you documented all deficiencies?

## Have you created remediation plans to address any deficiencies found in the audits?

- ☐ Are these remediation plans fully documented in writing?
- ☐ Do you update and review these remediation plans annually?
- ☐ Are annually documented remediation plans retained in your records for 6 years?

## Have all staff members undergone annual HIPAA training?

- ☐ Do you have documentation of their training?
- ☐ Is there a staff member designated as the HIPAA compliance, privacy, and/or security officer?

## Do you have policies and procedures relevant to annual HIPAA privacy, security, and breach notification rules?

- ☐ Do you have documentation of their training?
- ☐ Is there a staff member designated as the HIPAA compliance, privacy, and/or security officer?

## Have you identified all your vendors and business associates?

- ☐ Do you have business associate agreements in place with all business associates?
- ☐ Have you performed due diligence on your business associates to assess their HIPAA compliance?
- ☐ Are you tracking and reviewing your business associate agreement annually?
- ☐ Do you have confidentiality agreements with non-business associate vendors?

## Do you have a defined process for incidents or breaches?

- ☐ Do you have the ability to track and manage the investigation of all incidents?
- ☐ Are you able to provide the required reporting of minor or meaningful breaches or incidents?
- ☐ Do your staff members have the ability to anonymously report an incident?

## Is your infrastructure up to the challenge?

### Data Access Control

- ☐ Is physical access to your facility secured?
- ☐ Do you use unique identifiers for patients and business entities?
- ☐ Have you configured automatic session termination & access control on all computers, tablets and other devices?
- ☐ Are you using encryption everywhere you can, both for data in transit as well as at rest?

### Activity Auditing

- ☐ Do you have monitoring and logging of both successful and failed attempts at accessing data?
- ☐ Is that audit data secured and available only to those with a business need to access?
- ☐ Do you keep a history of changes tracking the movement of stored information?
- ☐ Are you regularly reviewing activity audits for suspicious access?

**User Authorization**

- ☐ Are you using secure passwords and secure password management practices, like the use of a password manager?
- ☐ Are credentials (such as logins for desktops, e-mail accounts, EMR systems) assigned to individual people, and not shared roles?
- ☐ Do you monitor and review access privileges regularly to ensure that authorized users have access only to the information they need?
- ☐ Do you have a documented process for on-boarding and off-boarding staff that includes the revocation of assigned credentials?
- ☐ Are you using two-factor authentication everywhere possible?
- ☐ Have the default passwords on all network devices been changed? Check routers, firewalls, printers and other devices carefully.
- ☐ Do you keep a history of changes tracking the movement of stored information?

**Infrastructure Planning**

- ☐ Do you track and ensure that all workstations, servers, network and firewall equipment and other IT equipment are continually patched and free of known vulnerabilities?
- ☐ Are you regularly auditing configuration and software on all these devices?
- ☐ Do you have a firewall?
- ☐ Does your wireless infrastructure segregate guests and non-business staff devices from your secure internal network?
- ☐ Do you have regular off-site encrypted backups of all stored information?
- ☐ Do you regularly audit backups to ensure that data is retrievable, and that all necessary data is being backed up?
- ☐ Are all devices encrypted at rest, using technologies like BitLocker? This is especially critical for laptops, portable hard drives and other easily removeable assets?

**Safe Data Transmission**

- ☐ Do you ensure the use of encrypted communication methods when transmitting PHI?
- ☐ Do you have strong technology controls to ensure that PHI is not sent using insecure communications channels?
- ☐ Are there mechanisms in place to ensure that non-secure devices cannot access PHI?

DID YOU KNOW: IF AUDITED, YOU MUST PROVIDE ALL DOCUMENTATION FOR THE PAST 6 YEARS TO AUDITORS.

## Do you need help?

Not every organization is able to devote a large share of their administrative or clinical resources to a HIPAA compliance effort, so retaining some outside help often makes business sense. County Micro is a managed IT services provider specializing in healthcare technology and network security. We help healthcare providers meet and exceed their HIPAA compliance obligations by taking a proactive, whole-of-organization approach to your IT needs.

*This checklist is composed of general questions about the measures your organization should have in place to state that you are HIPAA compliant, and does not qualify as legal advice. Successfully completing this checklist **does not** certify that you or your organization are HIPAA compliant.*

COUNTYMICRO
YOUR TRUSTED IT SOLUTIONS PARTNER

**Phone:** (207) 521-9190
**Address:** 135 Main St. Houlton, ME 04730-2418
**Email:** hello@countymicro.com
**Website:** countymicro.com