

# HIPAA CHECKLIST

## REQUIRED TRAINING

- All employees trained to 2020 HIPAA Standards
- All employees sign the **Proof-of-HIPAA Training Sheet**
- All employees sign the **Confidentiality/Non-Disclosure Agreement**
- All employees sign the **Employees Technology Use Agreement**
- All temporary employees and Volunteer Students sign **all of the above**
- Re-train all above if HIPAA laws change or if there are **HIPAA breach incidents during the year**

## REQUIRED DOCUMENTS

- 2020 HIPAA Manual or Update all written required protocols
- Customize HIPAA Manual on all required facility and training protocols
- List HIPAA officer and HIPAA advisory Committee on written documents (if applicable)
- Have written social media posting protocols/including a patient release for pictures
- Understand all marketing and product dispensing rules under the HIPAA Omnibus Rule
- Update all job descriptions to include current HIPAA-required standards
- Business Associate agreements, signed by appropriate vendors, kept on file
- Independent contractors sign Non-Disclosure agreements, kept on file
- Breach Reporting protocols written and understood by each employee
- Major vs. Minor HIPAA breaches clearly understood, and protocols to report
- Breach Assessment Form: Written and accessible to each employee

- All patients sign an updated HIPAA form written to current HIPAA law-update regularly
- Third Party Access to records documents updated for all patients regularly
- HIPAA Notice of Privacy Policies displayed in the office and on the practice website
- Medicare, Medicaid, and Healthy Kids programs; use required HIPAA documents and posters
- Annual data backup and contingency report: created and kept on file at least annually by data backup provider
- HIPAA Risk Assessment Report, created at least annually by the HIPAA Officer, kept on file
- Red Flag Rule for fraud prevention; highly recommended to be written protocols

## REQUIRED FACILITY PROTOCOLS

- Update all Windows-based software computer stations to the latest version of Windows by January 10
- Retire your take-home data backup drives (Use trusted encrypted cloud services)
- Get email encryption software for business email accounts
- Convert faxes to email
- Protect texting practices - do not include PHI or use encryption apps for cell phones
- Computer Screens: Keep all HIPAA screens in HIPAA mode, move away from patient viewing or use privacy screens
- Use only IT Techs that are proficient in HIPAA Omnibus Rule set up for Healthcare Standards
- Use PHI minimally, customize written protocols for your practice, destroy or lock up PHI
- Practice HIPAA breach reporting protocols and situational reactions

