HIPAA check-list

Required training

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

Required documents

- ○ Current 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 a written social media posting protocols/including patient release for pictures
- ○ Understand all marketing and product dispensing rules under 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 sing Non-Disclosure agreements, kept on file
- ○ Breach Reporting protocols written and understood by each employee
- ○ Major vs. Minor HIPAA breach 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 office and on practice website

- Medicare, Medicaid and Healthy Kids programs; use required HIPAA documents and posters
- Annual data back up and contingency report; created and kept on file at least annually by data back-up provider
- HIPAA Risk Assessment Report; created at least annually by HIPAA Officer, kept on file
- Red Flag Rule for fraud prevention; highly recommended to be written protocols

Required facility protocols

- Update all computer stations to latest windows/mac operating system
- Retire your take home data back-up 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 app for cell phones
- Computer Screens; Keep all HIPAA screens in HIPAA mode, 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