HIPAA Risk Assessment

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that you perform a periodic “risk assessment” of your practice. A risk assessment is a mandatory analysis of your practice that identifies the strengths and weaknesses of the safeguards your practice has in place to protect patient information and privacy. A risk assessment should include an evaluation of at least three types of safeguards you should use in your practice: (1) physical safeguards; (2) technical safeguards; and (3) administrative safeguards.

A risk assessment is a formal process and must be documented in writing. The risk assessment should include documented review of each type of safeguard, as well as any identified weaknesses and/or deficiencies of those safeguards in your practice. After you identify any existing weaknesses and/or deficiencies in your safeguards, you should either take the appropriate steps to address those weaknesses and/or deficiencies in your safeguards or document the reasons why you cannot reasonably address or implement those safeguards.

Remember, each practice is unique and a risk assessment must consider these differences in privacy and security needs, resources, and capabilities. For example, a risk assessment for a specialty surgical group comprised of 20 physicians may look very different from a risk assessment for a medical practice with two or three psychiatrists.

DISCLAIMER: THE FOLLOWING CHECKLIST IS ONLY INTENDED TO PROVIDE YOU WITH A GENERAL AWARENESS OF COMMON PRIVACY AND SECURITY ISSUES. IT IS NOT INTENDED IN ANY WAY TO BE AN EXHAUSTIVE OR COMPREHENSIVE RISK ASSESSMENT CHECKLIST. EACH RISK ASSESSMENT MUST BE TAILORED TO CONSIDER THE PRACTICE’S CAPABILITIES, RESOURCES, AND SITUATION AND MAY REQUIRE THAT YOU CONSIDER ADDITIONAL OR OTHER SPECIFIC OFFICE ISSUES AND SAFEGUARDS THAT ARE NOT LISTED BELOW.

Sample HIPAA Risk Assessment General Checklist

Physical Safeguards	
Office Access	
Is there a “gatekeeper” (e.g., receptionist) on duty to control access to the office during business hours?	□Yes □No
Are restricted office areas secured with locks or key card entry?	□Yes □No
Are all vendors escorted while visiting areas of the office?	□Yes □No
Is there a formal document retention and disposal policy for protected health information (PHI)?	□Yes □No
Does the office have access to and use cross-cut shredders for convenient disposal of paper records? Alternatively, does the office contract with off-site shredding services?	□Yes □No
How does the office dispose of electronic records (e.g., CDs, DVDs, hard drives)?	
Is there an exit interview or process to ensure return or destruction of all PHI upon termination/leave/resignation of office personnel?	□Yes □No
Office Workstations and Remote/Mobile Device Access	
Are office workstations (i.e., computers) restricted to office personnel (i.e., nurses, physicians, office assistants, PAs, etc.)?	□Yes □No
Is there an on-site server that stores PHI for the office? If so, is the server area locked or accessible only by designated office employees?	□Yes □No
Does the office use a cloud-based service or off-site server to store PHI for the office?	□Yes □No
Does the office dispose of or recycle old computers/hard drives/fax machines? Is the information contained on those old computers/hard drives wiped clean before disposal or recycling?	□Yes □No
Do office workstations/laptops use unique login/user names for each individual?	□Yes □No
Do office workstations require passwords?	□Yes □No
Emergency/Contingency Plans	
Is there a plan or service in place for back-up and recovery of PHI in the event of an emergency or disaster?	□Yes □No
Technical Safeguards	
Workstation Security and Encryption	
Do office workstations all have anti-virus software and use firewalls?	□Yes □No
Is the anti-virus software regularly updated?	□Yes □No
How complex are office workstation passwords?	
How often are workstation passwords required to be changed?	
Do office workstations time out and log out automatically after a period of inactivity?	□Yes □No
Remote and Mobile Access	
Does the office use laptops/tablets/mobile devices/flash drives to access office e-mails or PHI?	□Yes □No
Are the laptops/tablets/mobile devices secured with password protection? Are flash drives secured with encryption?	□Yes □No
Does the office have a method to track workstation access by office personnel?	□Yes □No
Does the office have the ability to terminate remote access to office workstations if laptops/tablets/mobile devices are stolen or lost?	□Yes □No

DISCLAIMER: THIS CHECKLIST IS ONLY INTENDED TO PROVIDE YOU WITH A GENERAL AWARENESS OF COMMON PRIVACY AND SECURITY ISSUES. IT IS NOT INTENDED IN ANY WAY TO BE AN EXHAUSTIVE OR COMPREHENSIVE RISK ASSESSMENT CHECKLIST. EACH RISK ASSESSMENT MUST BE TAILORED TO CONSIDER THE PRACTICE’S CAPABILITIES, RESOURCES, AND SITUATION AND MAY REQUIRE THAT YOU CONSIDER ADDITIONAL OR OTHER SPECIFIC OFFICE ISSUES AND SAFEGUARDS THAT ARE NOT LISTED BELOW.

Sample HIPAA Risk Assessment General Checklist

Does the office have the ability to remotely wipe office data and PHI from lost or stolen laptops/tablets/mobile devices?	□Yes □No
Does the office send e-mails with PHI to patients? Are e-mails with PHI encrypted? If not, are patients provided with confidentiality statements about the risks of unencrypted e-mails?	□Yes □No
Hospital/Medical Center	
Does anyone on your medical office staff (e.g., physicians or nurses) work at hospital(s) or in conjunction with outside medical groups?	□Yes □No
If so, does the hospital or outside medical group provide your medical staff with access to the hospital/medical group PHI network or system?	□Yes □No
Is your medical staff aware of the hospital/medical group's network or system access rules and requirements?	□Yes □No
Does your medical staff allow any other individuals (including other members of the office) to use his/her access to the network or system without the hospital/medical group's knowledge/consent?	□Yes □No
Administrative Safeguards	
Office Training and Awareness	
Has the office designated an individual to be in charge of HIPAA training?	□Yes □No
Has the office conducted a HIPAA risk assessment previously?	□Yes □No
Has the entire office had HIPAA training?	□Yes □No
How often does the office undergo HIPAA training?	
Has every member of the office reviewed and executed a confidentiality agreement?	□Yes □No
Reporting of Incidents	
Is there a policy or procedure for reporting potential office privacy or security incidents?	□Yes □No
Has the office received training on the recognition of potential privacy or security incidents?	□Yes □No
Vendor Contracts and Agreements	
Does the office use any outside vendors to provide any medical or support services to the office?	□Yes □No
If so, is there a written contract/agreement in place with these outside vendors?	□Yes □No
Do these contracts/agreements expressly address HIPAA privacy and security rule issues?	□Yes □No

Explain "No" Answers:

____

____

____

DISCLAIMER: THIS CHECKLIST IS ONLY INTENDED TO PROVIDE YOU WITH A GENERAL AWARENESS OF COMMON PRIVACY AND SECURITY ISSUES. IT IS NOT INTENDED IN ANY WAY TO BE AN EXHAUSTIVE OR COMPREHENSIVE RISK ASSESSMENT CHECKLIST. EACH RISK ASSESSMENT MUST BE TAILORED TO CONSIDER THE PRACTICE'S CAPABILITIES, RESOURCES, AND SITUATION AND MAY REQUIRE THAT YOU CONSIDER ADDITIONAL OR OTHER SPECIFIC OFFICE ISSUES AND SAFEGUARDS THAT ARE NOT LISTED BELOW.