HIPAA Compliance Checklist

This document is an abridged version of the checklist that can be found in APA's HIPAA resource document for members.

Although this abbreviated checklist is still many pages long, and some of the information will only be relevant to large medical practices with several auxiliary staff members, it should prove helpful as a reminder of the various areas in a practice where confidentiality issues may arise. An office that is concerned about maintaining confidentiality will find that most of the relevant areas are already complied with.

Front Office/Check-In

	Review of Current Procedure	**Guidelines for Policy Adherence**	**Action Needed to be Taken/Responsible** **Person/Date Completed**
Task 1	Does the practice use a patient sign in sheet?	If a sign-in sheet is used, the "minimum necessary" standard should be followed with sensitivity toward protecting individual health information (e.g., limit the sign-in sheet to the patient's name and date).	
Task 2	How does the practice obtain verification from an established patient that his/her demographic and insurance information is still accurate?	If this applies, have check-in receptionist provide a printed copy of patient's demographic and insurance information to the patient for his/her review. Request that the patient note any changes prior to returning it to the check-in receptionist.	
Task 3	If it is necessary for check-in staff to request verbal clarification of patient-related information, is a private area readily available to protect the patient's privacy during the verbal exchange (e.g., a cubicle or separate office)?	Voices should be kept down so that the conversation cannot be overheard easily by non-authorized persons. Alternatively, a private area should be established for staff to discuss protected health information (PHI) with patients in order to adhere to the minimum necessary release of information standard.	

Front Office/Check-In (continued)

	Review of Current Procedure	Guidelines for Policy Adherence	Action Needed to be Taken/Responsible Person/Date Completed
Task 4	Are computer screens visible to patients in the waiting area?	Computer screens should be facing away from patients and non-authorized individuals. As an alternative, screen covers that allow only straight-on viewing can be used to protect patient confidentiality.	
Task 5	A. If the practice maintains a website, is the practice's Notice of Privacy Practices prominently placed on the site and available for viewing? B. Is the patient provided with a copy of the practice's Notice of Privacy Practices describing the practice's uses and disclosures of PHI? C. Is written acknowledgement of receipt of the Notice of Privacy Practices obtained from the patient? D. Is the practice's Notice of Privacy Practices posted? If so, where?	All of these are required. See Notice of Privacy Protections.	
Task 6	How are patients called to the exam/treatment area?	To protect patient confidentiality, practices may wish to avoid using both first and last names together, and instead use either just first name or just last name when calling patients back for treatment or use.	
Task 7	A. Are messages left on answering machines/ voice mails? B. Are postcards used to remind patients of appointments? C. Do invoices or other correspondence to patients reflect on the exterior envelope the nature of the practice	Unless patients fill out a Request for Limitations and Restrictions of Protected Health Information form reasonable alternative means of communication or an alternative location at which to be contacted, practices may call patients and leave messages on answering machines/voicemails. Preferably, postcards should not be used to remind patients of appointments. Correspondence to patients should be labeled "Personal and Confidential" and if at all possible should not identify the nature of services offered by the practice.	

Front Office/General

	Review of Current Procedure	Guidelines for Policy Adherence	Action Needed to be Taken/Responsible Person/Date Completed
Task 1	Does the practice have protocols for verifying that a patient contacting the practice or a patient contacted by the practice via telephone for appointment scheduling, collections activities, communicating lab results, etc. is actually the patient in question?	The patient identity should be verified by DOB, social security number, mother's maiden name, PIN or other unique identifier. The patient should provide this confirming information, not the practice.	
Task 2	If PHI is received in the office via facsimile, is the fax machine located in a non-public, secure area?	Fax machines should be located away from areas where patients or other non-authorized individuals may be present or have visual access.	
Task 3	Does the practice verify that outgoing faxes are going to the appropriate party and confirming fax numbers of recipients?	Only parties authorized to receive PHI under applicable law and the practice's privacy policies should receive PHI via fax. All fax numbers should be confirmed prior to dialing, or use autodial features.	
Task 4	Are staff and/or providers logging out of all software programs prior to leaving computer terminal unattended?	All providers and staff should log out of all programs containing PHI prior to leaving a computer terminal unattended. The use of a password protected screensaver is another viable alternative.	
Task 5	Are all staff members provided with unique passwords for program access?	Each staff member and provider should immediately be provided with his/her own password that allows him/her access to PHI only at levels required by his/her job description in order to adhere to the minimum necessary standard.	

Medical Records

	Review of Current Procedure	Guidelines for Policy Adherence	Action Needed to be Taken/Responsible Person/Date Completed
Task 1	Who is authorized to access and/or remove medical records?	Define those authorized and permit only the personnel whose job description states that they need access to medical records to remove and file charts. (Regulation)	
Task 2	When medical records are removed from the filing system, is there a tracking mechanism in place to document the charts' location?	A tracking mechanism such as outguides or other devices should be used to track the whereabouts of medical records to aid in ensuring that PHI is only in authorized areas.	
Task 3	Has the practice determined the physical means of maintaining medical records so that they meet the privacy and security requirements?	Medical records must be kept private and secure. (Regulation) A suggestion would be to have an area for charts to be locked after hours. Another alternative would be to obtain a	

		confidentiality agreement with after-hours service providers.	
Task 4	Are medical records transported between locations?	Only PHI that is necessary for carrying out treatment, payment and other healthcare operations (TPO) should be transported to satellite locations. (Information needed should be copied, if possible, to prevent misplacing patients' medical record.) Note: If a courier is used, the PHI should not be visible/accessible to the courier. A suggestion would be to use a lock bag with couriers. Otherwise, be certain that a Business Associate Agreement is in place with the courier.	
Task 5	Does the practice have a process for using and disclosing PHI?	See Notice of Privacy Practices.	
Task 6	Is a patient's written authorization obtained (as appropriate) prior to releasing PHI for purposes other than TPO?	This is required.	
Task 7	Are signed authorizations to disclose PHI for reasons other than treatment, payment or healthcare operations (TPO) maintained in each patient's medical record?	This is required.	
Task 8	Does the practice have staff members who are trained to respond to patient's requests regarding their own PHI?	The practice must have at least one staff member who is knowledgeable and responsive to patients' inquiries about exercising their rights to restrict, amend, and obtain copies of or an accounting of disclosures of their PHI.	
Task 9	Does the practice contract with an outside vendor for the destruction of medical records that should be purged?	The practice is required to have a Business Associate Agreement with third party vendors who have access to PHI	
Task 10	When PHI is destroyed, is it burned, shredded or otherwise rendered unreadable?	PHI must be rendered unreadable when it is destroyed. Consider using a shredder to destroy documents.	
Task 11	If psychotherapy notes are retained in the patient record, are they segregated or identified so as to easily preclude unauthorized dissemination?	Any release of psychotherapy notes requires an authorization. (Regulation)	
Task 12	Does the practice communicate with patients via e-mail?	The practice should obtain patient per-mission and consider using encryption for e-mail messages with patients. The practice should establish policies to authenticate the recipients and senders of e-mail containing PHI. (Suggestion)	
Task 13	Do the providers take medical records out of the practice?	Except in emergencies related to patient care, providers should not take medical records out of the practice. The information that is taken out of the practice should be limited to only that which is needed to care for the patient.	
Task 14	Does the practice have a mechanism for de-identification of PHI?	See Document Determine Whether Your Practice Discloses PHI for Research Purposes for what to do in research situations.	

Task 15	Are deceased patients' records treated according to the same policy as current patients' records?	Deceased patients' records are subject to the same rules as all living patients; however, this requirement applies only for a period of fifty (50) years following the death of the individual. (Regulation)	

Business Associate

	Review of Current Procedure	**Guidelines for Policy Adherence**	**Action Needed to be Taken/Responsible** **Person/Date Completed**
Task 1	Are signed business associates agreements in place, if the practice utilizes any of the following and the entity needs access to PHI to perform services for the practice?	This is a requirement See form Business Associate Agreement (Regulation).	
Task 2	How do Business Associates identify themselves when visiting the practice (e.g., badge, business card, driver's license)?	Business Associate identities should be verified prior to giving access to the practice and PHI, in order to protect patient confidentiality.	

Personnel

	Review of Current Procedure	**Guidelines for Policy Adherence***	**Action Needed to be Taken/Responsible** **Person/Date Completed**
Task 1	Does the practice have written Privacy Policies and Procedures in place?	The practice must have written Privacy policies and procedures included in their policies and procedures manual.	
Task 2	Are the practice's Privacy Policies and Procedures periodically reviewed and updated? If so, how often? • If so, by whom? • If so, when were they most recently updated?	The practice should review their privacy policies and procedures at least annually and must update them as required if there are changes to the Privacy Rule. (Regulation)	
Task 3	Do new employees receive privacy training as part of their new employee orientation? Have all existing employees undergone training?	This is a requirement.	
Task 4	Has new employee privacy training taken place? Is it documented?	This is a requirement.	
Task 5	Does every practice employee have a signed workforce confidentiality agreement in his/her personnel file?	See Workforce Confidentiality Agreement.	