HIPAA Self-Assessment Worksheet

Part 2: Analyze the Data

Parts 1 and 2 of the *HIPAA Self-Assessment Worksheet* were created to help you identify areas where action might be needed to comply with HIPAA. The questions in this document may help you further analyze the data collected in Part 1.

DATE COMPLETED: _____ **COMPLETED BY:** _____

	YES	NO	COMMENTS
1) Steps have been taken to minimize the likelihood that patients and visitors can easily see or access computer screens/monitors and other records containing PHI. For example: ☐ Computer screens time out. ☐ Files are put away or turned over to avoid easy viewing. ☐ PDAs (hand-held computer devices) are kept in a secure manner by the authorized individual. ☐ Records, including CDs and DVDs, are stored in a secure manner. ☐ Other:_____			
2) Medical, financial, and other records containing PHI are secure and accessible only to those people employed by or doing work on behalf of the practice that have a legitimate—job-related—need to know; e.g., maintained in locked file cabinets or locked medical record rooms.			
3) Computers are password protected—each user has a unique identifier—and passwords are changed on a regular basis.			
4) Access controls (e.g., passwords, computer accounts, combinations, keys) to computers, filing cabinets, and the building are terminated or changed when employees or contract workers end their relationship with the practice.			
5) Electronic equipment and other records containing PHI are stored in a secure location to prevent theft or vandalism—using both physical security (e.g., alarms and locks) and electronic security (access controls, firewalls, and virus checks, all for which you should consider seeking technical expertise).			
6) Documents or records that contain patients' personal, financial, and health information—and are no longer needed—are destroyed. ☐ Shredded or ☐ Incinerated. ☐ Information is kept showing how, why, and by whom medical records were destroyed. ☐ Medical records are retained at least: • 6 years from the date of the patient's death. • 10 years from the date of the patient's last medical service. • 21 years from the date of a child's birth for pediatric records and for the obstetric patient's prenatal records, or 10 years after the minor patient's last medical service, whichever period is longer. ☐ Patient management systems data (financial, etc.) is retained for 10 years. ☐ Prior to sale or disposal of computer equipment that stores PHI, the hardware is completely erased by reformatting the hard drive. (Technical knowledge needed.) ☐ Other: _____			

This information is intended as advisory in nature and should not be considered as legal advice nor is it a substitute for legal advice. This information does not constitute technical information nor system/security advice. It is designed to assist you in your own risk management activities. It is not intended to be exclusively relied upon or used as a substitute for your own loss-control program. Accuracy and completeness are not guaranteed.

November 2009

	YES	NO	COMMENTS
7) Computer systems containing PHI have systems to protect data integrity and to prevent data loss, for example: ☐ Backup systems are used to prevent loss of data due to power outage, hackers, etc. ☐ Audit trails systems are periodically audited.			
8) Procedures address handling of medical, financial, or other records containing PHI—for example: ☐ Original records are handled correctly (e.g., not removed from premises and charted appropriately, including corrections). ☐ Patient requests for copying of and amendment to records are handled correctly. ☐ Patient requests for an accounting of disclosures of PHI are handled quickly and correctly. ☐ Message boards, daily patient schedules, etc., that allow viewing of patient financial or health information are maintained in areas restricted to employees who have a legitimate job-related need to know. ☐ Measures are taken to ensure that conversations held with patients concerning financial and health information maintain privacy. For example: • Exam room doors are closed. • Background music is used in waiting/reception areas to minimize the likelihood of overhearing PHI. • Solid core doors are used to minimize sound travel. • Phone messages are listened to in private. ☐ Steps are taken to reduce the likelihood that facsimile transmissions may be sent to an incorrect telephone number. For example: • Confidential disclaimer is utilized on facsimile or electronic transmission. • Transmissions are limited for urgent/emergent needs to transmit private health information. • Infrequently used fax numbers are verified prior to transmission. ☐ Cell phone conversations about patients that require the release of Individually Identifiable Health Information are conducted only to ensure continuity of care. ☐ Steps are taken to protect the privacy and security of information, if e-mail or another electronic form of communication is used to communicate personal health information.			
9) Staff—including volunteers—are trained in privacy and in maintaining the security of health information. Education is documented and includes: ☐ Appropriate handling of personal health information, including specific policies. ☐ Use of discretion when discussing personal health information within hearing of others. ☐ Use of discretion when leaving telephone and electronic messages for patients. ☐ Software password-security procedures. ☐ Signed confidentiality statements. ☐ Staff accountability for following procedures and applicable laws to protect privacy and security of PHI.			
10) Criminal security/background checks are conducted prior to hiring employees.			
11) Board members understand, and are trained in, maintaining the privacy and security of any PHI that they may have a legitimate need to know. And, they: ☐ Sign confidentiality agreements			

This information is intended as advisory in nature and should not be considered as legal advice nor is it a substitute for legal advice. This information does not constitute technical information nor system/security advice. It is designed to assist you in your own risk management activities. It is not intended to be exclusively relied upon or used as a substitute for your own loss-control program. Accuracy and completeness are not guaranteed.

	YES	NO	COMMENTS
12) Policies address appropriate handling of patient concerns—including concerns related to the privacy and security of PHI.			
13) Forms and documents that affect the use and disclosure of patient health information (e.g., IRB authorization) have been identified, reviewed for compliance with HIPAA, and modified as needed. Using the following list of forms, determine which forms you currently use that you will no longer need. a. *Employee Confidentiality and HIPAA Training Acknowledgment Statement* b. *Revocation of Authorization to Use or Disclose Protected Health Information* c. *Request to Correct or Amend Protected Health Information* d. *Authorization to Use or Disclose Protected Health Information* e. *Notice of Privacy Practices* Assess the remaining forms for HIPAA compliance.			
14) Business associates are expected to use reasonable measures to handle PHI in a private and secure manner. ☐ If written agreements exist, consult legal counsel to ensure HIPAA provisions are met. If written agreements do not exist, work with legal counsel to draft "*Business Associate Agreements*" required by HIPAA. ☐ Business associates, as appropriate, are educated about pertinent practices/policies pertaining to privacy and security when they have reason to perform any job-related functions on premises.			
15) List other areas pertaining to your operations affected by HIPAA and not listed in this document. a. _____ b. _____ c. _____			

If you responded with a "NO" to any item, further action may be necessary to provide reasonable protection for PHI.

You may want to use the *HIPAA Self-Assessment Worksheet Part 3: Action Plan* to document your actions, rationale behind your plan, and follow-up.

This information is intended as advisory in nature and should not be considered as legal advice nor is it a substitute for legal advice. This information does not constitute technical information nor system/security advice. It is designed to assist you in your own risk management activities. It is not intended to be exclusively relied upon or used as a substitute for your own loss-control program. Accuracy and completeness are not guaranteed.

HIPAA Self-Assessment Worksheet
Part 3: Action Plan

Using Parts 1 and 2 of the *HIPAA Self-Assessment Worksheet*, identify each issue that might require further action to comply with HIPAA.
Then use this or a similar form to develop an action plan by documenting each issue, its action plan, the reason for your decision, your follow-up, and the responsible individual.

ISSUE	ACTION PLAN (Circle all changes that you plan to implement, and attach estimated costs)	REASON FOR DECISION (Check all that apply)	FOLLOW-UP	RESPONSIBLE PARTY
1.) Information overheard in waiting room	System/equipment change — background music - stereo system New policy/policy change New form/form change Job description change Education — completed 9/1/09 Facility upgrade Other:	☑ Options selected provide reasonable protections of PHI. ☑ Options not feasible at this time: upgrade on hold - budget ☐ Other:	☐ Date Completed: ___/___/___ ☑ Monitor ☑ Budget for: $2000.00 stereo in 2010 (budget year)	Cathy
2.) Disposal of confidential information	System/equipment change New policy/policy change New form/form change Job description change Education — scheduled 10/1/09 Facility upgrade Other:	☑ Options selected provide reasonable protections of PHI. ☑ Options not feasible at this time: ☑ Other:	☑ Date Completed: 10 / 1 / 09 ☑ Monitor ☐ Budget for: in (budget year)	Pat
3.) Sensitive information discussed on phone - possibility of being overheard	System/equipment change — (see issue #1 action plan) New policy/policy change New form/form change Job description change Education — completed 8/1/09 Facility upgrade Other:	☑ Options selected provide reasonable protections of PHI. ☑ Options not feasible at this time: upgrade on hold - budget ☑ Other:	☐ Date Completed: ___/___/___ ☑ Monitor ☑ Budget for: $2000.00 stereo in 2010 (budget year)	Cathy

This information is intended as advisory in nature and should not be considered as legal advice nor is it a substitute for legal advice. This information does not constitute technical information nor system/security advice. It is designed to assist you in your own risk management activities. It is not intended to be exclusively relied upon or used as a substitute for your own loss-control program. Accuracy and completeness are not guaranteed.

HIPAA Self-Assessment Worksheet
Part 3: Action Plan

Using Parts 1 and 2 of the *HIPAA Self-Assessment Worksheet*, identify each issue that might require further action to comply with HIPAA.
Then use this or a similar form to develop an action plan by documenting each issue, its action plan, the reason for your decision, your follow-up, and the responsible individual.

ISSUE	ACTION PLAN (Circle all changes that you plan to implement, and attach estimated costs)	REASON FOR DECISION (Check all that apply)	FOLLOW-UP	RESPONSIBLE PARTY
4.) PHI left on the counter – accessible to unauthorized persons	System/equipment change New policy/policy change New form/form change Job description change (Education) move information to restricted area ASAP Facility upgrade Other:	☑ Options selected provide reasonable protections of PHI. ☑ Options not feasible at this time: ☐ Other:	☑ Date Completed: 10 / 1 / 09 ☑ Monitor ☐ Budget for: in (budget year)	Kathy
5.) Files with PHI accessible to unauthorized persons	System/equipment change New policy/policy change New form/form change Job description change (Education) Facility upgrade Other:	☑ Options selected provide reasonable protections of PHI. ☐ Options not feasible at this time: ☑ Other:	☑ Date Completed: 10 / 1 / 09 ☐ Monitor ☐ Budget for: in (budget year)	Dave
6. a) computer screens visible to patients b) patients may access network	(System/equipment change) Program for passwords and add screen savers New policy/policy change New form/form change Job description change (Education) of policy changes Facility upgrade Other: assess computer system - possible upgrade	☑ Options selected provide reasonable protections of PHI. ☑ Options not feasible at this time: assessment of computer on hold due to budget ☑ Other:	☐ Date Completed: / / ☑ Monitor ☑ Budget for: Assessment upgrade in 2010 (budget year)	Kim

This information is intended as advisory in nature and should not be considered as legal advice nor is it a substitute for legal advice. This information does not constitute technical information nor system/security advice. It is designed to assist you in your own risk management activities. It is not intended to be exclusively relied upon or used as a substitute for your own loss-control program. Accuracy and completeness are not guaranteed.

HIPAA Self-Assessment Worksheet
Part 3: Action Plan

Using Parts 1 and 2 of the *HIPAA Self-Assessment Worksheet*, identify each issue that might require further action to comply with HIPAA.
Then use this or a similar form to develop an action plan by documenting each issue, its action plan, the reason for your decision, your follow-up, and the responsible individual.

ISSUE	ACTION PLAN (Circle all changes that you plan to implement, and attach estimated costs)	REASON FOR DECISION (Check all that apply)	FOLLOW-UP	RESPONSIBLE PARTY
7.) need business associate agreements: • Transcription • Accountant • Collection agency	System/equipment change New policy/policy change New form/form change Job description change Education Facility upgrade (Other:) obtain sample business assoc. agreements	☑ Options selected provide reasonable protections of PHI. ☐ Options not feasible at this time: _____ ☐ Other: _____	☐ Date Completed: ___/___/___ ☐ Monitor ☑ Budget for: Legal review in 2010 (budget year)	Dennis
	System/equipment change New policy/policy change New form/form change Job description change Education Facility upgrade Other: _____	☐ Options selected provide reasonable protections of PHI. ☐ Options not feasible at this time: _____ ☐ Other: _____	☐ Date Completed: ___/___/___ ☐ Monitor ☐ Budget for: _____ in _____ (budget year)	
	System/equipment change New policy/policy change New form/form change Job description change Education Facility upgrade Other: _____	☐ Options selected provide reasonable protections of PHI. ☐ Options not feasible at this time: _____ ☐ Other: _____	☐ Date Completed: ___/___/___ ☐ Monitor ☐ Budget for: _____ in _____ (budget year)	

This information is intended as advisory in nature and should not be considered as legal advice nor is it a substitute for legal advice. This information does not constitute technical information nor system/security advice. It is designed to assist you in your own risk management activities. It is not intended to be exclusively relied upon or used as a substitute for your own loss-control program. Accuracy and completeness are not guaranteed.

HIPAA Self-Assessment Worksheet

Part 3: Action Plan

Using Parts 1 and 2 of the *HIPAA Self-Assessment Worksheet*, identify each issue that might require further action to comply with HIPAA. Then use this or a similar form to develop an action plan by documenting each issue, its action plan, the reason for your decision, your follow-up, and the responsible individual.

ISSUE	ACTION PLAN (Circle all changes that you plan to implement, and attach estimated costs)	REASON FOR DECISION (Check all that apply)	FOLLOW-UP	RESPONSIBLE PARTY
	System/equipment change New policy/policy change New form/form change Job description change Education Facility upgrade Other: ____________________	☐ Options selected provide reasonable protections of PHI. ☐ Options not feasible at this time: ____________ ____________ ☐ Other: ____________ ____________	☐ Date Completed: ____/____/____ ☐ Monitor ☐ Budget for: ____________ in ____________ (budget year)	
	System/equipment change New policy/policy change New form/form change Job description change Education Facility upgrade Other: ____________________	☐ Options selected provide reasonable protections of PHI. ☐ Options not feasible at this time: ____________ ____________ ☐ Other: ____________ ____________	☐ Date Completed: ____/____/____ ☐ Monitor ☐ Budget for: ____________ in ____________ (budget year)	
	System/equipment change New policy/policy change New form/form change Job description change Education Facility upgrade Other: ____________________	☐ Options selected provide reasonable protections of PHI. ☐ Options not feasible at this time: ____________ ____________ ☐ Other: ____________ ____________	☐ Date Completed: ____/____/____ ☐ Monitor ☐ Budget for: ____________ in ____________ (budget year)	

This information is intended as advisory in nature and should not be considered as legal advice nor is it a substitute for legal advice. This information does not constitute technical information nor system/security advice. It is designed to assist you in your own risk management activities. It is not intended to be exclusively relied upon or used as a substitute for your own loss-control program. Accuracy and completeness are not guaranteed.

November 2009