HIPAA Risk Assessment and Action Plan

Date: _____

In order to comply with the HIPAA Security Rule, all covered providers must have regular risk assessments to ensure that their patients' private health information (PHI) is as safe as possible. Here is a sample risk analysis you can use that is based upon a document from HHS designed to help small providers with HIPAA security compliance. We all make changes in our offices that can result in compromising the security of patients' information; regular risk assessments help us ensure that we keep the information as safe as possible.

The standard requires that we regularly assess administrative, technical and physical safeguards to ensure compliance with the HIPAA rules. This form will help you perform regular checks. Please note, some of these items are considered "required" and some are "addressable"; in other words, some of them you have to do, and some of them need to be considered to see if they are the best way to protect PHI. It gives us a great starting place, and a good checklist, to ensure that we're considering many areas that could cause issues.

Please note this is a sample risk analysis that you may use to formulate your own policies and risk assessments, and may not cover every situation that may exist in every office. Always check with your own attorney or malpractice carrier to make sure your assessment is complete. (*You may also use the government's free risk assessment tool: https://www.healthit.gov/providers-professionals/security-risk-assessment-tool to help you ensure that your risk assessment is as complete as possible*.)

Please fill out this form. For any actions that need to be performed, number the item, and at the end, fill out the actions that must be taken for each numbered item on the attached action plan. **MAKE SURE YOU FIX ANY PROBLEMS YOU FIND TO AVOID POTENTIALLY SEVERE PENALTIES in the event of a problem!!!**

Contact info for computer security questions/concerns/issues: (name/phone #): _____

	Yes	No	Needs to be addressed	Item # on action plan
General office information/Administrative safeguards				
Have you conducted a thorough risk analysis to determine potential risks and vulnerabilities to the safety of patient's electronic private health information (PHI)?				
Do you perform annual risk assessments to discuss new issues and to ensure PHI is as safe as possible?				
Does your risk assessment help identify threats to PHI and prevent impermissible uses and disclosures?				
Do you perform monthly assessments to make sure nothing has changed that could affect patient privacy/computer security?				
Do you perform a risk assessment if there is a significant change in policies or in the business environment?				
Are breach analyses performed in the event of a possible breach and the results recorded in the manual?				
Do you have a security and/or privacy officer in charge of the HIPAA program? Name(s):				
Are there adequate numbers of employees to help with HIPAA implementation duties if it's too much for one individual?				
Is that person able to develop, implement, and document new privacy and security policies and procedures, as needed?				

	Yes	No	Needs to be addressed	Item # on action plan
Is that person qualified to access security protections (call the computer guy) and serve as the contact person for problems with policies/procedures/monitoring/training/patient complaints?				
Do you know where PHI is located in the office? Please underline all that apply: desktop computer , laptop computer, tablets, smartphones, server, flash drive, removable hard drives, CDs, paper charts, other: _____				
Do you have a current inventory of all devices/technical items that may contain patients' PHI?				
If devices leave the office, is a list of their locations maintained?				
Do you know the approximate value of all technical items that may contain patients' PHI?				
Do you classify your electronic PHI as having low/medium/high impact if you're unable to use them?				
Do you have a current backup in the event of a natural disaster so that your patients' information can be easily restored and can you access the information, if needed?				
Do you have control over the information on your computer system?				
Do you have a HIPAA manual and is all documentation about Privacy and Security policies and procedures stored and retained in the manual?				
Are all paper products/xrays/etc. that contains PHI shredded/destroyed before disposal?				
Are all devices containing PHI properly destroyed/disposed of when they are no longer used? Is the process documented?				
If applicable, do you have a log for those accessing your facility?				
Business Associates (BA)				
Does any vendor or business associate have access to your computer system?				
Does any vendor or business associate have the ability to access and change confidential patient data? If so, are audit logs monitored to prevent unauthorized access?				
Do you have **business associate agreements in place for all vendors** who may have access to your patients' PHI?				
Do these agreements have assurances that these business associates will properly protect patients' information using proper privacy and security safeguards?				
Do you use a clearinghouse, and if so, do they take precautions to protect your patients' information during processing and transmission?				
Do business associates know they must immediately inform your office in the event of a breach?				
Do these agreements include indemnification agreements in the event a breach is caused by a BA? Do they have insurance?				
Do you have policies in place to recover data and restrict further use of PHI if a business associate is terminated?				
Employee Information				
Have your employees received training on basic HIPAA requirements (Privacy, Security, HITECH, and Omnibus Acts)?				
Do you provide additional training if policies and procedures are changed and implemented?				
Do you document all employees training?				
Do you have written policies and procedures that explain employee requirements under HIPAA, including which job titles have access to PHI?				
Do you contact references and/or conduct background checks before hiring employees?				

	Yes	No	Needs to be addressed	Item # on action plan
Do employees know where the HIPAA manual is kept and who is the HIPAA officer?				
Do all employees understand there are specific sanctions for violating HIPAA Privacy and Security policies (including being fired) and that all sanctions will be enforced?				
Do all employees understand that, in addition to workplace sanctions, they can also be fined and imprisoned for deliberately violating HIPAA rules?				
Do only those employees, who need access to patients' PHI, actually have access to PHI? (Policies and procedures should ensure that those without authorization, should not be able to access patients' information)				
Does each employee have a specific log in ID and understand they can be sanctioned if they share passwords?				
Do you use passwords on your system to prevent unauthorized access?				
Are employees trained not to share passwords or leave them in places that are easily accessible? (no sticky notes!)				
If you have any employees who are not authorized to access some/all patients' PHI, could they access it?				
If an employee is terminated, is the employee's access to the office and computer system immediately terminated? (return keys, change passwords, return all devices, change passwords/logins, etc.)? Are business associates notified, as needed?				
Do you periodically review employees' access to PHI as needed? (If they change to a job that no longer requires access to patients' PHI, they should no longer have access)				
If any employees can access your system using their personal devices, are their devices protected (encryption, etc.)?				
If any security/privacy lapses among employees occur, is additional training and instruction provided and sanctions applied?				
Do new employees receive training about the HIPAA programs and are informed about policies, sanctions, etc.?				
Do employees know to inform the HIPAA officer immediately if they suspect information has been compromised?				
General computer protection information				
Would you know if someone was trying to hack into your system? (Do you get alerts-ask your computer guy)				
Do you have audit logs that may show unsuccessful log-ins or other indicators of unauthorized access?				
Does everyone have a unique password and are they protected and changed when indicated?				
In the event of computer destruction or loss or evidence of a computer security incident, are there policies and procedures to restore computer service and restore data (and does everyone know who to call)?				
Do employees know they should not install personal software, surf the internet, access social media, or access personal e-mails on the office computer system because of the potential for viruses and malware?				
If you offer patients Wi-Fi in your office, is their access on a separate router to prevent access to your system?				
Is your network properly protected? Are all workstations attached to the proper (protected) network?				
Do you perform regular risk assessments, policy and procedure evaluations, and security evaluations, at least annually and/or any time a change is made?				
Do you have firewalls, anti-viral software, etc. to protect your information from malware/spyware/viruses? (If you use a computer expert, have him write a summary of precautions you've taken to place in your HIPAA manual)				
Is all security related software and hardware evaluated regularly and updated as needed?				
Are any security incidents/possible security events evaluated and documented?				
Do you backup your data? Do you have a system to restore your backup if your system was destroyed?				
Is your phone system properly protected? (VoIP systems should be HIPAA compliant; regular phone systems don't require encryption. Consult with your computer expert to make sure your phone system is properly protected)				

	Yes	No	Needs to be addressed	Item # on action plan
Evaluate your phone system to make sure stored texts voicemails are adequately protected and establish procedures on how to handle them. (Consult computer expert to determine what level of protection is best for your system.)				
Is your data stored offsite in the event the office is destroyed? (What if your home is destroyed at the same time? You should have data backed up in a manner that will provide for widespread devastation to a large area.)				
Do you have a plan that will allow you to temporarily relocate if your office is damaged and is everyone aware of the plan?				
In the event you're in a temporary location, could patients' information be adequately protected?				
Do you have copies of existing software, or a method to install software, in the event you have to replace a computer?				
If you make changes to your computer system or relocate computers in the office, do you evaluate the situation to ensure that the new changes do not compromise security? (For example, you move a computer to a consult room and patients may have unsupervised access in that room; passwords, etc. would be very important on that computer).				
Do you have procedures in place in the event of a ransomware attack?				
Do you regularly restore your backup to ensure that data is actually being backed up correctly? (Ransomware hackers will often send a virus that makes it look like you're backing up your data, but you're not)				
Are employees informed about phishing and told not to open any attachments/documents they are not expecting?				
Since each employee has a unique identifier in the computer system, could their activities be tracked in the system?				
Do you use e-mail in the office to transmit PHI and is it encrypted? (check with your computer guy)				
Are systems in place to ensure that photos/xrays are on encrypted devices only and are not being uploaded to a cloud storage system that may not be properly encrypted? (Do not take patient pictures on personal phones)				
Are other methods of protecting documents, such as password protection of individual documents, used?				
Physical Safeguards				
Do you have a written plan listing security measures?				
Is your facility protected from unauthorized physical access? (Do you have door locks, cameras, alarms, physical safeguards preventing computer removal, locked cabinets, etc?)				
Are computers secured and access limited to employees with proper permission?				
Do you use screen savers, privacy screens, etc. to ensure that patient information isn't easily visible to others?				
Are computers placed to ensure that patients' PHI isn't easily visible to others?				
Are computers placed to ensure that unauthorized people don't have unsupervised access? (And if they are unsupervised, is there adequate protection to ensure that other patients' information can't be accessed?)				
Do unattended computers automatically log off when not being used so access isn't available?				
If computers or electronic media are no longer being used/are being replaced, is there a method that destroys the data before disposal? (destroy hard drive, professionally wipe the hard drive so data can't be recovered, etc.)				
On all equipment (faxes/copiers/medical equip, etc) is memory cleared before they are disposed of/returned/removed?				
Are all flash drives, hard drives, etc. all accounted for and it is known who has them in their possession at all times?				
Is data consistently backed up?				
If data is backed up to a physical item such as a CD or flash drive, are they encrypted? How are they protected, stored and destroyed?				

	Yes	No	Needs to be addressed	Item # on action plan
Technical Safeguards				
If a patient requests information and the doctor/employee doesn't have access to the encrypted email address to transmit the information, do the doctor and employees know they can request patient permission to transmit using an unencrypted e-mail and then transmit only if permission is granted? (*save record of transmission*)				
If a patient requests access or a copy to PHI, is his/her identification verified?				
Are users denied access after a certain number of failed log-in attempts?				
Does the doctor and/or security officer know how to conduct audits for altered information, failed log-ins, etc.?				
Are charts or electronic devices ever taken out of the office (including backup devices, smartphones, laptops, tablets, etc.)? If so, do employees know how to safeguard info? (use secure networks, etc.)				
Are all devices that contain, or can access, PHI properly encrypted? (backup devides, smartphones, laptops, tablets, etc.)				
Is your electronic PHI protected by encrypting your information? (Encryption is the only method that will actually render electronic information "unusable" which can avoid a breach in the event your information is accessed, lost, or stolen.)				
If your information is not encrypted, do you have encrypted passwords (If it's determined that's sufficient protection)?				
Are any electronic portable devices that can access patients' information encrypted? (smartphones, laptops, etc.)				
Do your employees know to immediately report any suspected breaches of information?				
Do your business associates know to immediately report any suspected breaches of information and provide you with all needed information to determine if a breach has occurred?				
Do your business associate agreements have specifics about how breaches will be handled, and are indemnification agreements in place to ensure that notification and mitigation costs will be covered?				
General Privacy Provisions				
Do employees understand the necessity of disclosing the "minimum amount necessary"?				
Is there personal health information on the outside of patients' charts?				
Are paper charts inaccessible to unauthorized people?				
Are paper charts stored in a secure area to prevent theft or destruction?				
Is all paper containing PHI shredded before disposal?				
Do you control who can amend your patient records?				
If sensitive matters are discussed, is there a place to take patients for a more confidential discussion? (Note: never close yourself in a room with just you and a patient. Always bring in another person or leave the door cracked and put someone outside the door to protect you from any false claims or accusations.)				
Do employees know never to discuss patients outside the office?				
Do you have authorizations so you can discuss PHI matters with those who are financially responsible for others?				
Are schedules posted in a non-obvious location?				
On sign in sheets, do you ensure that no personal information is asked such as "what is your dental problem today"?				
Is the "Notice of Privacy Policies" posted and available to patients, and did patients sign a form acknowledging receipt?				
Do employees understand that PHI cannot be used for personal reasons?				
Have patients signed authorizations for any photos/xrays/videos/social media postings used in your office and are all reviews on social media answered using approved comments only? (before/after pictures, pictures on facebook, YELP etc.)				
Before complying with subpoenas, legal requests, do you check with your attorney to ensure you're complying with HIPAA?				

Action Plan

Item # on Risk Analysis	Actions that need to be taken	Date Completed

Item # on Risk Analysis	Actions that need to be taken	Date Completed

<u>IT Asset Inventory</u>

(Please note that this is a sample inventory for a smaller dental practice with a simple computer setup. Llarger practices with many devices may want to use a spreadsheet to keep this current, plus they may want to include more information. Talk to your computer dude to make sure that the information in your inventory is current and complete for your office situation)

Description*	Manuf/Model	Serial #	Location	Patient info stored on the device?	Approx Cost

What programs are installed on the computer system?

Program used on computer	Do you have disk to install the program, or is it installed online, or is it a subscription service?

Please note: *Medical devices that store patient information should have independent risk assessments to make sure they aren't exposing the network to cyber attacks. In hospitals, for example, these devices have been shown to be very susceptible to cyber attacks, so check with your computer guys to ensure that these devices are properly secured.