Risk Assessments Result

General Office Information	
Have you conducted a thorough risk analysis to determine potential risks and vulnerabilities to the safety of patient's electronic private health information (PHI)?	Yes
Do you have a security and/or privacy officer in charge of the HIPAA program?	Yes
Do you know where PHI is located in the office?	Yes
Do you have a current inventory of all technical items that may contain patients' PHI?	Yes
Do you know the approximate value of all technical items that may contain patients' PHI?	Yes
Have you taken reasonable security measures to protect your patient's information, including door locks, the use of passwords, security systems, and other measures to ensure that PHI is secured?	Yes
Do you have a current backup in the event of a natural disaster so that your patients' information can be easily restored?	Yes
Do you have control over the information on your computer system?	Yes
How do you plan on addressing any potential risks?	By planning and implementing activities, programs, procedures or other control methods.
Business Associates	
Does any vendor or business associate have access to your computer system?	No
Does any vendor or business associate have the ability to access and change confidential patient data?	No
Do you have business associate agreements in place for all vendors who may have access to your patients' PHI?	Yes
Do these agreements have assurances that these business associates will properly protect patients' information?	Yes
Do these agreements include indemnification agreements in the event a breach is caused by a business associate?	Yes
How do you plan on addressing any potential risks?	By planning and implementing activities, programs, procedures or other control methods.
Employee Information	
Have your employees received training on basic HIPAA requirements (Privacy, Security, HITECH, and Omnibus Acts)?	Yes
Do you provide additional training if new policies and procedures are implemented?	Yes
Do you document all employees training?	Yes
Do you have written policies and procedures that explain employee requirements under HIPAA?	Yes
Do you contact references and/or conduct background checks before hiring employees?	Yes
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?	Yes
Do all employees understand that, in addition to workplace sanctions, they can also be fined and imprisoned for deliberately violating HIPAA rules?	Yes
Do only those employees, who need access to patients' PHI, actually have access to PHI? (Those without authorization, should not be able to access patients' information)	Yes
Does each employee have a specific log in ID?	Yes
Do you use passwords on your system to prevent unauthorized access?	Yes
Are employees trained not to share passwords or leave them in places that are easily accessible?	Yes
If you have any employees who are not authorized to access patients' PHI, could they access it?	No
Do terminated employees still have access to your computer system	No
Do you have systems in place to prevent that scenario?	Yes
Are locks/passwords/etc. changed to prevent continued facility access after termination?	Yes
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)	Yes
If any employees can access your system using their personal devices, are they aware of encryption requirements?	N/A

If any security/privacy lapses among employees occur, is additional training and instruction provided?	Yes
Do new employees receive training about the HIPAA programs and are informed about policies, sanctions, etc.?	Yes
Do employees know to inform the HIPAA officer immediately if they suspect information has been compromised?	Yes
How do you plan on addressing any potential risks?	By planning and implementing activities, programs, procedures or other control methods.

General computer protection information

Would you know if someone was trying to hack into your system?	Yes
Do you have audit logs that may show unsuccessful log-ins or other indicators of unauthorized access?	Yes
Are passwords protected and changed when indicated?	Yes
In the event of computer destruction or loss, are there policies and procedures to restore computer service and restore data (does everyone know who to call)?	Yes
Do employees know they should not install personal software or access personal e-mails on the office computer system because of the potential for viruses and malware?	Yes
If you offer patients Wi-Fi in your office, is their access on a separate router to prevent access to your system?	N/A
Do you perform regular risk assessments and security evaluations, at least annually or any time a change is made?	Yes
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)	Yes
Are any security incidents documented?	Yes
Do you backup your data?	Yes
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.)	Yes
Do you have a plan that will allow you to temporarily relocate if your office is damaged?	Yes
In the event you're in a temporary location, could patients' information be adequately protected?	Yes
Do you have copies of existing software in the event you have to replace a computer?	Yes
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).	Yes
How do you plan on addressing any potential risks?	By planning and implementing activities, programs, procedures or other control methods.

Physical Safeguards

Is your facility protected from unauthorized physical access? (Do you have door locks, cameras, alarms, physical safeguards preventing computer removal, locked cabinets, etc?)	Yes
If hardware, doors, locks, walls, etc. are repaired or modified, are any changes that could affect the security of PHI should be documented?	Yes
Do you use screen savers, privacy screens, etc. to ensure that patient information isn't easily visible to others?	Yes
Are computers placed to ensure that patients' PHI isn't easily visible to others?	Yes
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?)	Yes
Do unattended computers automatically log off when not being used?	Yes
If computers or electronic media are no longer being used/are being replaced, is there a method that destroys the data before disposal?	Yes
Are all flash drives, hard drives, etc. all accounted for and it is known who has them in their possession at all times?	N/A
Is data consistently backed up?	Yes

If data is backed up to a physical item such as a CD or flash drive, how are they protected, stored and destroyed?	No data is saved on portable media, only on network servers accessed via zero client workstations.
How do you plan on addressing any potential risks?	By planning and implementing activities, programs, procedures or other control methods.

Technical Safeguards

Since each employee has a unique identifier in the computer system, could their activities be tracked in the system?	Yes
Are passwords unique and not shared?	Yes
Are employees notified that they may be sanctions if they share passwords or use someone else's identifier?	Yes
Do employees have access to only the minimum PHI necessary to do their job duties? (This is usually not relevant in most dental offices where those who have access need access to everything; however, some larger practices do have separate departments for billing, etc.)	Yes
If specific emergency procedures are in place that require certain codes for PHI access, are the codes protected and available only to those who need them?	Yes
If you have automatic logoff for computers, does the time before it logs off shorten for those computers in high traffic areas?	Yes
Do you use e-mail in the office to transmit PHI?	No
Do you have a method to encrypt e-mails if it's used to transmit PHI?	N/A
Are other methods of protecting documents, such as password protection of individual documents, used?	N/A
Are users denied access after a certain number of failed log-in attempts?	Yes
Does the doctor and/or security officer know how to conduct audits for altered information, failed log-ins, etc.?	Yes
Are charts or electronic devices ever taken out of the office (including backup devices, smart phones, etc.)?	No
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.)	Yes
If your information is not encrypted, do you have encrypted passwords?	Yes
Are any electronic portable devices that can access patients' information encrypted?	N/A
Do your employees know to immediately report any suspected breaches of information?	Yes
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?	Yes
How do you plan on addressing any potential risks?	By planning and implementing activities, programs, procedures or other control methods.

General Privacy Provisions

Do employees understand the necessity of disclosing the "minimum amount necessary"?	Yes
Is there personal health information on the outside of patients' charts?	N/A
Are paper charts inaccessible to unauthorized people?	N/A
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.)	N/A
Do employees know never to discuss patients outside the office?	Yes
Are schedules posted in a non-obvious location?	N/A
On sign in sheets, do you ensure that no personal information is asked such as "what is your dental problem today"?	N/A
Is the "Notice of Privacy Policies" posted and available to patients, and did patients sign a form acknowledging receipt?	Yes
Do employees understand that PHI cannot be used for personal reasons?	Yes
Have patients signed authorizations for any photos/xrays used in your office? (before/after pictures, etc.)	N/A

How do you plan on addressing any potential risks?

By planning and implementing activities, programs, procedures or other control methods.