Security Risk Analysis

Risk analysis and **risk management** may be performed by reviewing and answering the following questions and keeping this review (with date and signature) for evidence of this analysis. The following table lists risk analysis questions, information, and suggestions provided by ChiroTouch. Complete this questionnaire each year, and save it in your records. CMS can audit your compliance up to six years after a reporting period.

Risk Analysis

Risk Analysis Question	ChiroTouch Information	Comments
What new electronic health information has been introduced into my practice because of EHRs? Where will that electronic health information reside?	Electronic health information in the EHR system is protected following ONC-ATCB security guidelines.	
Who in my office (employees, other providers, etc.) will have access to EHRs, and the electronic health information contained within them?	Designated administrators will set permissions within the software to manage access to electronic health information.	
Should all employees with access to EHRs have the same level of access?	Each employee should have a unique access level decided upon by the administrator.	
Will I permit my employees to have electronic health information on mobile computing/storage equipment? If so, do they know how, and do they have the resources necessary, to keep electronic health information secure on these devices?		
How will I know if electronic health information has been accidentally or maliciously disclosed to an unauthorized person?	The ChiroTouch audit log can be routinely reviewed to view actions performed within the software.	
When I upgrade my computer storage equipment (e.g., hard drives), will electronic health information be properly erased from the old storage equipment before I dispose of it?		
Are my backup facilities secured (computers, tapes, offices, etc., used to backup EHRs and other health IT)?	CTSecure can be implemented to securely backup health information off-site. If you do not already have this service, contact your Account Manager for more information.	
Will I be sharing EHRs, or electronic health information contained in EHRs with other health care entities through a HIO (Health Information Exchange)? If so, what security policies do I need to be aware of?		
If my EHR system is capable of providing my patients with a way to access their health record/information via the Internet (e.g., through a portal), am I familiar with the security requirements that will protect my patients electronic health information before I implement that feature?	ChiroTouch ONC-ATCB certification ensures that the software meets all security, integrity, and data exchange guidelines.	

Will I communicate with my patients electronically (e.g., through a portal or email)? Are those communications secured?	Patient communication through the Patient Portal is secured via private patient password.	
If I offer my patients a method of communicating with me electronically, how will I know that I am communicating with the right patient?	Patient authentication is verified upon entry into the patient portal.	
Questions to Ask Yourself When Assessing Integrity Risks		
Who in my office will be permitted to create or modify an EHR, or electronic health information contained in the EHR?	Access may be provided to those the administrator deems should have access.	
How will I know if an EHR, or the electronic health information in the EHR, has been altered or deleted?	All activity in a chart is recorded in the audit log for review.	
If I participate in a HIO (Health Information Exchange), how will I know if the health information I exchange is altered in an unauthorized manner?		
If my EHR system is capable of providing my patients with a way to access their health record/information via the Internet and I implement that feature, will my patients be permitted to modify any of the health information within their record? If so, what information?	The patient portal allows patients read-only rights.	
Questions to Ask Yourself When Assessing Availability Risks		
How will I ensure that electronic health information, regardless of where it resides, is readily available to me and my employees for authorized purposes, including after normal office hours?		
Do I have a backup strategy for my EHRs in the event of an emergency, or to ensure I have access to patient information if the power goes out or my computer crashes?	CTSecure can be implemented to securely backup health information off-site. If you do not already have this service, contact your Account Manager for more information.	
If I participate in a HIO, does it have performance standards regarding network availability?		
If my EHR system is capable of providing my patients with a way to access their health record/information via the Internet (e.g., through a portal) and I implement that feature, will I allow 24/7 access?		

____

Signature of Administrator

____

Date

Risk Management

Risk Management Question	ChiroTouch Information	Comments
Questions to Ask Yourself When Identifying Technical Safeguards		
Have I updated my internal information security processes to include the use of EHRs, connectivity to HIOs, offering portal access to patients, and the handling and management of electronic health information in general?		
Have I trained my employees on the use of EHRs? Other electronic health information related technologies that I plan to implement? Do they understand the importance of keeping electronic health information protected?	Find additional training on MyChiroTouch, including videos and documentation.	
Have I identified how I will periodically assess my use of health IT to ensure my safeguards are effective?	Implement a protocol for routine assessment and sign/date those assessments.	
As employees enter and leave my practice, have I defined processes to ensure electronic health information access controls are updated accordingly?		
Have I developed a security incident response plan so that my employees know how to respond to a potential security incident involving electronic health information (e.g., unauthorized access to an EHR, corrupted electronic health information)?	The audit log helps manage EHR system use. Review these logs and follow HIPAA guidance if patient records are breached.	
Have I developed processes that outline how electronic health information will be backed-up or stored outside of my practice when it is no longer needed (e.g., when a patient moves and no longer receives care at the practice)?		
Have I developed contingency plans so that my employees know what to do if access to EHRs and other electronic health information is not available for an extended period of time?	This is your responsibility. You need to have a plan in place for backing up your data. You need to develop your own contingency plan in preparation for the possibility that your software or hardware is nonfunctional for an extended period of time.	
Have I developed processes for securely exchanging electronic health information with other health care entities?		
Have I developed processes that my patients can use to securely connect to a portal? Have I developed processes for proofing the identity of my patients before granting them access to the portal?	Access to the patient portal is patient-designated password-protected.	
Do I have a process to periodically test my health IT backup capabilities, so that I am prepared to execute them?		
If equipment is stolen or lost, have I defined processes to respond to the theft or loss?		

Questions to Ask Yourself When Identifying Physical Safeguards		
Do I have basic office security in place, such as locked doors and windows, and an alarm system? Are they being used properly during working and non-working hours?		
Are my desktop computing systems in areas that can be secured during non-working hours?	Verify the location of your computers are consistent with HIPAA compliance.	
Are my desktop computers out of the reach of patients and other personnel not employed by my practice during normal working hours?	Verify the location of your computers are consistent with HIPAA compliance.	
Is mobile equipment (e.g., laptops), used within and outside my office, secured to prevent theft or loss?		
Do I have a documented inventory of approved and known health IT computing equipment within my practice? Will I know if one of my employees is using a computer or media device not approved for my practice?	Keep an inventory list of your practice's electronic equipment.	
Do my employees implement basic computer security principles, such as logging out of a computer before leaving it unattended?	Automatic log-off may be set in the system via the CTLauncher options screen.	
Questions to Ask Yourself When Identifying Technical Safeguards		
Have I configured my computing environment where electronic health information resides using best-practice security settings (e.g., enabling a firewall, virus detection, and encryption where appropriate)? Am I maintaining that environment to stay up to date with the latest computer security updates?		
Are there other types of software on my electronic health information computing equipment that are not needed to sustain my health IT environment (e.g., a music file sharing program), which could put my health IT environment at risk?		
Is my EHR certified to address industry recognized/best-practice security requirements?	ChiroTouch is ONC-ATCB certified to address these requirements.	
Are my health IT applications installed properly, and are the vendor recommended security controls enabled (e.g., computer inactivity timeouts)?		
Is my health IT computing environment up to date with the most recent security updates and patches?		
Have I configured my EHR application to require my employees to be authenticated (e.g., username/password) before gaining access to the EHR? And have I set their access privileges to electronic health information correctly?		

If I have or plan to establish a patient portal, do I have the proper security controls in place to authenticate the patient (e.g., username/password) before granting access to the portal and the patient’s electronic health information? Does the portal’s security reflect industry best-practices?	Patient access is granted via an e-mail verification and patient password.	
If I have or plan to set up a wireless network, do I have the proper security controls defined and enabled (e.g., known access points, data encryption)?		
Have I enabled the appropriate audit controls within my health IT environment to be alerted of a potential security incident, or to examine security incidents that have occurred?		

____

Signature of Administrator

____

Date