

Risk Analysis

Confidentiality			
Question	default	Comments	Reviewed
What new electronic health information has been introduced into my practice because of EHRs? Where will that electronic health information reside?	Local web-connected computers have no PHI on them. The data is stored in a secure hosted environment that meets all the ONC-ACTB criteria. Be aware when a word document is created, it can be saved on the device, delete temp files		
Who in my office (employees, other providers, etc.) will have access to EHRs, and the electronic health information contained within them?	Those designated as Administrators will create access and set permissions for all other users.		
Should all employees with access to EHRs have the same level of access?	Each employee in a practice has unique and individual permissions, as set by the Administrator. These permissions govern features available to the user.		

<p>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?</p>	<p>No Internet-connected computer or device houses PHI locally. There is no local data to keep secure. Exception: scanned documents will be created on local computers, that need uploading to the web EHR system. Once uploaded, the local copy of these scanned image files should be deleted. Instruct users with Mobile devices to be aware of using the device in public places when accessing the HER</p>		
<p>How will I know if electronic health information has been accidentally or maliciously disclosed to an unauthorized person?</p>	<p>A designated person in the practice can review the Audit Log for the practice, or for a specific patient, at any time.</p>		

<p>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?</p>	<p>Make sure to dispose of devices properly.</p>		
<p>Are my backup facilities secured (computers, tapes, offices, etc., used to backup EHRs and other health IT)?</p>	<p>The web-based EHR manages all data backup. There are no local backups needed.</p>		
<p>Will I be sharing EHRs, or electronic health information contained in EHRs with other health care entities through a Health Exchange? If so, what security policies do I need to be aware of?</p>	<p>Data that is shared through a health exchange is encrypted.</p>		
<p>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?</p>	<p>eCWis ONC-ACTB Certified to meet all the security and data-exchange standards specified. The portal utilizes the same level of encryption, authentication, and integrity- checking.</p>		
<p>Will I communicate with my patients electronically (e.g., through a portal or email)? Are those communications secured?</p>	<p>Patient communications through the portal are secured. Discuss with your providers and staff you don't communicate PHI through personal email.</p>		

<p>If I offer my patients a method of communicating with me electronically, how will I know that I am communicating with the right patient?</p>	<p>Patient authentication on login to the PHR identifies the patient uniquely. Communication of any messages from/to this patient is ensured by the tight EHR-PHR linkage.</p>		
---	--	--	--

Integrity

Question	default	Comments	Reviewed
Who in my office will be permitted to create or modify an EHR, or electronic health information contained in the EHR?	The clinician can create and edit chart notes. Once signed, no one can alter them, though addenda can be appended.		
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 an Audit Log, which is a plain-English record of access, modification and deletion of data in a chart.		
How will I know if the health information I exchange is altered in an unauthorized manner in the eEHX.	External data imported into the EHR is kept separately from in-practice created data. All data, in-house and imported, is tracked in the Audit Log		

Availability			
Question	default	Comments	Reviewed
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?	With eCW, access can be achieved from any Internet-connected computer, from any location, at any time. No locally- installed client software is needed.		
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?	Nimbus is used in case the system breaks down, make sure that you have registered for Nimbus. If power goes out locally uses mobile devices.		
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?	Patient access to their PHR is web-based and on-demand, 24/7. Any secure communication between the clinician and patient will have response expectations set by notifications within the product. Do you allow patients to ask questions via the web?		

Attachment B: Identifying Safeguards

Administrative safeguards			
Question	default	Comments	Reviewed
Have I updated my internal information security processes to include the use of EHRs, connectivity to the eEHX, offering portal access to patients, and the handling and management of electronic health information in general?	Periodic review of the Risk Analysis, with comments and check / sign / date of each item accomplishes this.		
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?	Employees are inserviced on privacy and security tools available through the CIQN website. Employee sanction policy is reviewed with each employee, and placed in personnel record.		
Have I identified how I will periodically assess my use of health IT to ensure my safeguards are effective?	Establish periodicity by in- house policy, and conduct review of Identifying Safeguards. Check / sign / date each item to document this.		

<p>As employees enter and leave my practice, have I defined processes to ensure electronic health information access controls are updated accordingly?</p>	<p>Practice Administrator will manage the user list within the EHR, and will de-activate access to former employees.</p>		
<p>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)?</p>	<p>Only one instance of a user's login is supported at a time, so any login using stolen credentials can be identified. If EHR access using stolen credentials is identified, the practice will:</p> <ol style="list-style-type: none"> 1. Reset the password for that user, or de-activate that user 2. Review the Audit Logs to identify patients accessed by that user 3. Notify the patients whose records were breached within 30 days, in compliance with HIPAA standards 		
<p>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)?</p>	<p>Patients can be flagged as Inactive, as needed.</p>		

<p>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?</p>	<p>Since eCW is web-based, Internet connectivity is required. If there is a lapse in Internet connection from the main source, alternate methods of access will be implemented (e.g. wireless cell phone access), as technology allows.</p>		
<p>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?</p>	<p>The patient must then change his/her password upon first usage.</p>		
<p>Do I have a process to periodically test my health IT backup capabilities, so that I am prepared to execute them?</p>	<p>eCW is web- hosted on commercial-grade secured servers. Data backup is done centrally, and no local backup of data is needed.</p>		
<p>If equipment is stolen or lost, have I defined processes to respond to the theft or loss?</p>	<p>Since no PHI is contained on local computers, the loss or theft of equipment is simply property loss. Property loss is managed through routine theft-and-loss processes (e.g. police reporting, insurance reporting).</p>		

Physical safeguards

Question	PF default	Comments	Reviewed
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?	Practice manager to address and verify this.		
Are my desktop computing systems in areas that can be secured during non-working hours?	eCW implements auto-logout after a period of inactivity. However, the entire computer desktop should be Locked at the end of a work session.		
Are my desktop computers out of the reach of patients and other personnel not employed by my practice during normal working hours?	Verify physical location of computers, make sure screens are not visible by those not working at the station.		
Is mobile equipment (e.g., laptops), used within and outside my office, secured to prevent theft or loss?	eCW implements auto-logout after a period of inactivity. Upon leaving the premises, computers should be shut down or hibernated, with password re-launch required.		

<p>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?</p>	<p>With eCW, any Internet-connected computer can be used to connect to the EHR. Per-user access (regardless of physical machine or location) is captured in the Audit Log. It is good business practice to inventory in-house equipment.</p>		
<p>Do my employees implement basic computer security principles, such as logging out of a computer before leaving it unattended?</p>	<p>eCW implements auto-logout after a period of inactivity. However, the entire computer desktop should be Locked at the end of a work session.</p>		

Technical safeguards			
Question	PF default	Comments	Reviewed
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?	<p>eCW maintains security on the server. There is no local PHI.</p> <p>Exception: local copies of scanned-document files, and local copies of Reports that may have been output may contain PHI. They should</p> <ol style="list-style-type: none"> 1. Be deleted when finished with them 2. Should only be on machines with up-to-date antivirus and firewall software installed 3. If these files are to remain on a local machine, the files should be encrypted 4. Delete TIF files 		
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?	Since eCW is accessed through a simple web browser, and no local PHI resides on the client machine, there is no limitation to other software that may reside on that client machine.		

Is my EHR certified to address industry recognized/best-practice security requirements?	eCW is ONC-ACTB Certified to conform to industry recognized best- practice with respect to security.		
Are my health IT applications installed properly, and are the vendor recommended security controls enabled (e.g., computer inactivity timeouts)?	Only a web browser (any browser, any platform) with an Internet connection is required for eCW.		

Is my health IT computing environment up to date with the most recent security updates and patches?	Up to date security on any local client machine is advised. However, access to PHI via the eCW web browser is secured by the server and forces the browser to implement secure communication methods.		
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?	eCW requires a password, unique for each user, in order to access the system. Only one such session can be active at any given time. The Practice Administrator sets (and edits) permissions for each user in the practice		

<p>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?</p>	<p>Patient access to their PHR is granted one-at-a-time, via verified patient email. One of the three credentials needed for patient access is given to the patient in-person, and the remaining two credentials are emailed. The patient must then change his/her password upon first usage.</p>		
<p>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)?</p>	<p>Since eCW is web-based, all access is secured over the Internet. Local in-house wireless access is no different than access from home, or elsewhere, and needs no extra security layer in order to achieve a secure connection.</p>		
<p>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?</p>	<p>Periodic review of the Audit Log will be implemented and documented.</p>		

Attachment D: Audit Log review

Audit Log Review			
Date Audit Log was reviewed	Name of reviewer	Findings	Action needed
