practice fusion™
Free, web-based Electronic Health Records

Privacy and Security Toolkit

Documentation needed for conducting EHR security risk analysis

Action items

In order to conduct a **Security Risk analysis**, you need to do 4 things:

1. Conduct a Risk Analysis
2. Do a Risk Management Assessment
3. Implement an Employee Sanction Policy
4. Perform a periodic system activity review

If you are interested in more details on this, see the Overview section of this document. Otherwise, skip to the following sections:

1. **Print out this document** (particularly the Appendices A, B, C and D)
    a. Keep your printout on file, in case of an audit asking you to "prove that you did the security and risk analysis"
2. **Do the Risk Analysis**, use Appendix A
    a. Read each item, look at the default Practice Fusion answers to each question. Add comments if desired (can leave it blank). Sign or **initial**, and **date** each item (4th column).
3. **Do the Risk Management Assessment**, use Appendix B
    a. This has 4 sections. For each section, read each item, look at the default Practice Fusion answers. Add comments if desired. Sign or **initial**, and **date** each item (4th column).
4. **Include an Employee Sanction Policy** in your employment policy documents. For guidance, you can use a sample policy found in Appendix C
5. **Conduct a Periodic Audit.** We suggest at least monthly, but preferably weekly, you do the following:
    a. Look at the Practice Fusion audit log (the Activity Feed, under the Home tab). See if there are any irregularities, unauthorized access, or other issues.
    b. Fill in a row in the Audit Log (Appendix D), with the date of the review, the name/initials of the reviewer, any findings (e.g. "none"), and actions needed (e.g. "none").
    c. Add a new row with each audit. Weekly is suggested.

Congratulations!

Once you've done this, you can Attest to having done a Privacy and Security Audit. Keep your printouts in case of audits by CMS later on.

Overview

Introduction

Ensuring privacy and security of electronic health information is:

- Required by HIPAA,
- addressed by Office of the National Coordinator(ONC) via the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information,
- a Meaningful Use requirement.

The Meaningful Use objective is:

> Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities

The specific Meaningful Use measure is:

> Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

There are no exclusions to this measure. Everyone must conduct a review. The ONC has published a resource, the Small Practice Security Guide, which can be helpful.

Security Risk Analysis rules

The security risk analysis specified in the Meaningful Use measure is as follows:

45 CFR 164.308 - Administrative safeguards.

TITLE 45 - PUBLIC WELFARE
SUBTITLE A - DEPARTMENT OF HEALTH AND HUMAN SERVICES
CHAPTER I - SERVICES, GENERAL ADMINISTRATION
SUBCHAPTER C - ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS
PART 164 - SECURITY AND PRIVACY
subpart c - SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

164.308 - Administrative safeguards.

(a) A covered entity must, in accordance with 164.306:

(1)

(i) Standard:

Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) **Risk analysis** (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) **Risk management** (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).

(C**) Sanction policy** (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) **Information system activity review** (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Practice Fusion EHR

The Practice Fusion EHR is ONC-ACTB Certified for all the Certification criteria associated with the Meaningful Use measure.

The Certification criteria for this Meaningful Use Measure are as follows:

§170.302 (o)	**Access control**
§170.302 (p)	**Emergency access**
§170.302 (q)	**Automatic log-off**
§170.302 (r)	**Audit log**
§170.302 (s)	**Integrity**
§170.302 (t)	**Authentication**
§170.302 (u)	**General encryption**
§170.302 (v)	**Encryption when exchanging electronic health information**

By using Practice Fusion, many of the risks that a practice has with respect to maintaining personal health information (PHI) are minimized.

Conducting a risk assessment (Meaningful Use requirement)

Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the *confidentiality*, *integrity*, and *availability* of electronic protected health information held by the covered entity.

Definitions of the terms in the regulation:

- *Confidentiality* – the property that electronic health information is not made available or disclosed to unauthorized persons or processes.

- *Integrity* – the property that electronic health information have not been altered or destroyed in an unauthorized manner.
- *Availability* – the property that electronic health information is accessible and useable upon demand by an authorized person.

The ONC resource lists a series of "Questions to Ask Yourself" for each of these areas – confidentiality, integrity and availability. These can be assembled into a Checklist, and each item addressed – appended as ***Attachment A: Risk Analysis***.

Reviewing and checking answers to each of these items constitutes good-faith efforts to demonstrate a security risk review, and will stand as evidence supporting attestation of the Meaningful Use criterion. We suggest the practice print out the attachments, check, sign and date them, and keep them for reference.

Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).

The security standard referenced here is as follows:

164.306 - Security standards: General rules.

(a) *General requirements.* Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

The ONC resource lists a series of "Questions to Ask Yourself" around identifying safeguards for electronic health information in the realms of:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

These can be assembled into a Checklist, and each item addressed – appended as ***Attachment B: Identifying Safeguards***.

Reviewing and checking answers to each of these items constitutes good-faith efforts to demonstrate a risk management review, and will stand as evidence supporting attestation of the Meaningful Use criterion. We suggest the practice print out the attachments, check, sign and date them, and keep them for reference.

Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

- A practice should create an employee policy with regards to implementing sanctions against any failure to comply with the security policies identified above. A sample policy is attached as ***Attachment C: Sanction Policy (sample)***

  The sample Sanction Policy is adapted from a brief published by the American Health Information Management Association (AHIMA) IN 2009.

Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

- A practice should periodically review the Audit log contained in the Practice Fusion product, and document any findings. A sample record to document this review is attached as ***Attachment D: Audit Log review***

Attachment A: Risk Analysis

Confidentiality			
Question	**PF 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		
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.		
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?	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.		
How will I know if electronic health information has been accidentally or maliciously disclosed to an unauthorized person?	A designated person in the practice can review the Audit Log for the practice, or for a specific patient, at any time.		

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?	With a web-based EHR, no PHI is stored locally. Upgrading local machines does not leave any PHI exposed.		
Are my backup facilities secured (computers, tapes, offices, etc., used to backup EHRs and other health IT)?	The web-based EHR manages all data backup. There are no local backups needed.		
Will I be sharing EHRs, or electronic health information contained in EHRs with other health care entities through a HIO? If so, what security policies do I need to be aware of?	Data that is shared through a Health Information Exchange will be via security policies stated in the product, and which much be agreed to in order to access these services.		
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?	The entire Practice Fusion EHR platform is ONC-ACTB Certified to meet all the security and data-exchange standards specified. The connected PHR (Patient Fusion) utilizes the same level of encryption, authentication, and integrity-checking that the EHR does.		
Will I communicate with my patients electronically (e.g., through a portal or email)? Are those communications secured?	Patient communications through the linked PHR platform are secured. No PHI will be exposed through unsecured email.		
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 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.		

Integrity

Question	PF 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.		
If I participate in a HIO, how will I know if the health information I exchange is altered in an unauthorized manner?	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		
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 my patients be permitted to modify any of the health information within their record? If so, what information?	Clinician-created data, and patient-created data are kept separately. All activity, whether clinician-created or patient-created, is tracked in the Audit Log.		

Availability

Question	PF 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 a web-based EHR, access can be achieved from any Internet-connected computer, from any location, at any time. No locally-installed client software is needed. No VPN or other special connectivity 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?	Since the EHR is hosted on commercial-grade secure servers, up-time is ensured per the Service Level Agreement. Any local computer can be used to access this service, and local computer failure can be interchanged with any other computer.		
If I participate in a HIO, does it have performance standards regarding network availability?	The Practice Fusion web hosting system is run on commercial-grade servers, protected by a Service Level Agreement.		
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.		

Attachment B: Identifying Safeguards

Administrative safeguards			
Question	**PF default**	**Comments**	**Reviewed**
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?	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?	Each user undergoes training within the product, and can elect to engage online training and support with Practice Fusion (offered free). 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.		
As employees enter and leave my practice, have I defined processes to ensure electronic health information access controls are updated accordingly?	Practice Administrator will manage the user list within the EHR, and will de-activate access to former employees.		

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)?	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: 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		
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)?	The hosted EHR can store patient information *ad infinitum*, and manages all backup. No local backup is needed. Patients can be flagged as Inactive, as needed.		
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?	Since the EHR 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.		
Have I developed processes for securely exchanging electronic health information with other health care entities?	External electronic data exchange will occur only through the channels allowed within the product. Security for this exchange is documented within the product, and referenced in the Licencing Agreements.		

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?	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.		
Do I have a process to periodically test my health IT backup capabilities, so that I am prepared to execute them?	Practice Fusion is web-hosted on commercial-grade secured servers. Data backup is done centrally, and no local backup of data is needed.		
If equipment is stolen or lost, have I defined processes to respond to the theft or loss?	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).		

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?	Practice Fusion implements auto-logoff 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?	Practice Fusion implements auto-logoff after a period of inactivity. Upon leaving the premises, computers should be shut down or hibernated, with password re-launch required.		
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?	With Practice Fusion, 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, and is advised.		
Do my employees implement basic computer security principles, such as logging out of a computer before leaving it unattended?	Practice Fusion implements auto-logoff after a period of inactivity. However, the entire computer desktop should be Locked at the end of a work session.		

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?	The Practice Fusion EHR maintains security on the server. There is no local PHI. **Exception**: local copies of scanned-document files, and local copies of Reports that may have been output may contain PHI. They should 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		
Are their 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 Practice Fusion 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?	Practice Fusion 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 Practice Fusion.		

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 Practice Fusion 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?	Practice Fusion requires 3-key authentication, 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		
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 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. The PHR uses the same secure web server system that the Practice Fusion EHR uses, and is certified to conform to the same level of privacy and security that the EHR implements		

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)?	Since the Practice Fusion EHR 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.		
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?	Periodic review of the Audit Log will be implemented and documented.		

Attachment C: Sanction Policy (sample)

Medical practice name: ____

It is in the best interest of the healthcare industry generally, and this practice in particular, to address the issue of securing the Privacy and Security of individually-identifiable health information in a proactive manner through implementation of sanction practice standards. Aside from the necessity to ensure patient privacy as an ethical obligation, it is smart business. Data breach notification laws in more than 40 states require an organization to notify breach victims, which can damage its reputation.

Privacy Incident categories:

The practice defines categories that define the significance and impact of the privacy or security incident to help guide corrective action and remediation.

- **Category 1:** Unintentional breach of privacy or security that may be caused by carelessness, lack of knowledge, or lack of judgment, such as a registration error that causes a patient billing statement to be mailed to the wrong guarantor.
- **Category 2a:** Deliberate unauthorized access to PHI without PHI disclosure. Examples: snoopers accessing confidential information of a VIP, coworker, or neighbor without legitimate business reason; failure to follow policy without legitimate reason, such as password sharing.
- **Category 2b:** Deliberate unauthorized disclosure of PHI or deliberate tampering with data without malice or personal gain. Examples: snooper access and redisclosure to the news media; unauthorized modification of an electronic document to expedite a process.
- **Category 3:** Deliberate unauthorized disclosure of PHI for malice or personal gain. Examples: selling information to the tabloids or stealing individually identifiable health information to open credit card accounts.

Factors that may modify application of sanctions:

Sanctions may be modified based on mitigating factors. Factors may reflect greater damage caused by the breach and thus work against the offender and ultimately increase the penalty.

Examples include:

- Multiple offenses
- Harm to the breach victim(s)
- Breach of specially protected information such as HIV-related, psychiatric, substance abuse, and genetic data
- High volume of people or data affected
- High exposure for the institution
- Large organizational expense incurred, such as breach notifications
- Hampering the investigation
- Negative influence of actions on others

Factors that could mitigate sanctioning could include:

- Breach occurred as a result of attempting to help a patient
- Victim(s) suffered no harm
- Offender voluntarily admitted the breach and cooperated with the investigation
- Offender showed remorse
- Action was taken under pressure from an individual in a position of authority
- Employee was inadequately trained

Sanction process

The HIPAA regulations require that imposed sanctions be consistent across the board irrespective of the status of the violator, with comparable discipline imposed for comparable violations. This practice will enable application of general principles that will lead to fair and consistent outcomes.

Sanction implementation will follow the following steps. However, depending on the Category level of the incident, an escalated process can be followed if cause is shown:

- Documented conference with recommendations for additional, specific, documented training, if necessary
- First written warning (and training, as above, if warranted)
- Final warning, with or without suspension, with or without pay (training included, if warranted)
- Severance of formal relationship: employment, contract, medical staff privileges, volunteer status

Attachment D: Audit Log review

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