THE DARK SIDE OF ELECTRONIC HEALTH RECORDS
MEDICAL MALPRACTICE LIABILITY

Gerald E Meltzer, MD MSHA
Medical Director
iMedicWare

ASOA 2014

The following Medical eRisk Considerations were developed by the ***iHealth Alliance*** *and are provided for informational purposes only.*

The use of Electronic Health Records (EHRs) and online services is increasingly common in everyday physician practice. The unique concerns and risks inherent in this form of communication have prompted the development of the "Medical eRisk Considerations." The Medical eRisk ("Electronic Risk") Considerations were initially created in 2000 by the eRisk Working Group for Healthcare, a consortium including professional liability carriers, medical societies, and state licensing boards.

These Considerations are meant to serve as general suggestions and do not serve as professional advice of any kind. Clinicians are advised and encouraged to conduct their own independent research and seek further guidance on any specific questions or issues related to the subject matter herein from independent professionals. Full or partial adherence with any of these considerations imposes no obligation on any of the members of the eRisk Working Group, the iHealth Alliance or any other person or entity to offer any benefits of any kind to Clinicians such as lowering premiums, provide coverage of any claims, or offer any other benefits.

The Medical eRisk Considerations stress the following critical factors:

- Maintain patient confidentiality, privacy, security and authentication. Know and follow state and federal laws regarding patient privacy. Prevent unauthorized access.
- Obtain informed consent for online services; privacy protocols; and privacy rights.
- Limit online communications to existing patients.
- Discourage use of online communications for medical emergencies. Understand social media liability risks.
- Understand state licensing jurisdiction regarding online communication outside your state. Understand your responsibility for educational materials provided online to your patient.
- Document all online patient communications in the medical record – even "deleted" information is discoverable. Manage your fee-based consultations – charging can raise expectations re quality and thoroughness.
- You are responsible for the information shared with patients on your practice Web site – is it accurate and current? Verify on-line pharmacies through the Verified Internet Pharmacy Practice Sites program: http://www.nabp.net/programs/accreditation/vipps/
- Use extra caution when using online services to diagnose and treat new conditions.

- **Personal Health Records:** Patient responsibility for content and for informing you of important changes.

EHR Liability Risks

- You are responsible for patient medical information to which you have reasonable access – from whatever source. Know the source of your e-Prescribing Drug Information and Clinical Decision Support – ensure they comply with your specialty standards and have the full updated FDA approved labels and alerts.

- EHR patient questionnaires may use automated algorithms that record issues requiring your follow-up.

- Use caution when overriding or disabling alerts, warnings, reminders and embedded practice guidelines – "Alert Fatigue."
- Use caution in copying and pasting patient notes – avoid incorrect information in your EHR. Auto-populated fields may lead to incorrect patient information being recorded in the EHR.
- All your interactions with the EHR are time/date tracked and discoverable. Read your EHR contract carefully, particularly regarding liability.
- Don't allow the computer to become a barrier between you and your patients.

The Medical eRisk Considerations were initially developed by the *eRisk Working Group for Healthcare*, a consortium of professional liability carriers, medical societies and state licensure board representatives. They are meant to provide information to healthcare providers related to the use of electronic clinical systems, including Electronic Health Records (EHRs), and online communication and services with patients.

These Considerations are meant to serve as general suggestions and do not serve as professional advice of any kind. Clinicians are advised and encouraged to conduct their own independent research and seek further guidance on any specific questions or issues related to the subject matter herein from independent professionals. Full or partial adherence with any of these considerations imposes no obligation on any of the members of the eRisk Working Group, the iHealth Alliance or any other person or entity to offer any benefits of any kind to Clinicians such as lowering premiums, provide coverage of any claims, or offer any other benefits.

General Principles

The legal rules, ethical guidelines and professional etiquette that govern and guide traditional treatment and communications between the healthcare provider and patient are equally applicable to EHRs, email, Web sites, list serves, Personal Health Records (PHRs), social media and other electronic services and communications. However, this technology introduces special concerns and risks as follows:

1. Confidentiality. The healthcare clinician is responsible for protecting patient privacy and guarding against unauthorized access to and/or use of patient healthcare information. This responsibility extends to the use of network services that have an appropriate level of privacy and security as required under HIPAA. Following are key considerations: **a. Privacy and Security.** Online communications between healthcare clinicians and patients should be conducted over a secure network, with provisions for privacy and security, including encryption, in accordance with HIPAA. Standard email services do not meet the requirements under HIPAA.

Note: With respect to email specifically, clinicians are encouraged to add a disclosure to the bottom of their standard, non-secure email service stating that "this email is not secure, and is not for use by patients or for healthcare purposes in general."

b. Authentication. Healthcare clinicians have responsibility for taking reasonable steps to authenticate the identity of correspondent(s) in electronic communication and to ensure that recipients of information are authorized to receive it. Authentication of the patient or an authorized patient proxy (i.e., parent of a minor, authorized family member, etc.) for patient-provider online communication including the delivery of patient data is important in order to ensure patient privacy and confidentiality. Clinicians are encouraged to follow these suggestions for patient authentication:

i. Have a written patient authentication protocol for all practice personnel and require them to understand and adhere to it.

ii. Establish minimum standards for patient authentication when a patient is new to a practice or not well known.

iii. Keep an electronic or paper record of each patient authenticated for online communication or data exchange. The record should include the following:

1. Name of the patient

2. Date of authentication

3. Name of practice staff authenticating the patient

4. Means used to authenticate the patient

iv. Providers should not offer, promote or encourage patients to participate in online healthcare services where patient authentication is not addressed.

2. Unauthorized Access to Computers. Unauthorized physical access to computers can compromise patient information. Practices should establish procedures to guard against unauthorized access to computers with technologies such as automatic log-out and password protection.

3. Informed Consent. Prior to the initiation of online communication between healthcare clinician and patient, informed consent should be obtained regarding the appropriate use and limitations of this form of communication. Clinicians should develop written protocols for online communications, such as avoiding emergency use, heightened consideration of use for sensitive medical topics, and setting expectations for response times. Clinicians should also exercise discretion when selecting patients for the use of online services to ensure that they are capable of electronic communication and will be compliant. These guidelines should be documented in the clinician's practice policy manuals.

4. Pre-Existing Clinician-Patient Relationship. Healthcare clinicians may increase their liability exposure by initiating a clinician-patient relationship online. Online communications of any kind are best suited for patients previously seen and evaluated in an office setting.

5. Licensing Jurisdiction. Online interactions between a healthcare clinician and a patient are subject to requirements of state licensure. Communications online with a patient, outside of the state in which the clinician holds a license, may subject the clinician to increased risk. For example, pathologists, radiologists and other clinicians interpreting specimens, slides or images sent through interstate commerce for a primary diagnosis that becomes part of the patient's medical record should have a license to practice medicine in the state in which the patient presents for diagnosis or where the specimen is taken or the image is made. Intra-specialty consultation generally does not require in-state licensure, provided the consultation is requested by a physician licensed within the state and referenced in a report he or she issues. Physicians are advised to check with their medical board to determine licensure requirements.

6. Sensitive Subject Matter. Clinicians should advise patients of the risks that information the patient may consider sensitive might be inadvertently accessed by someone not authorized to see it, such as information on mental health, substance abuse, reproductive history, sexually transmitted diseases, drug and alcohol problems, genetic disorders and HIV status.

• Some states have laws about special classes of health information, such as HIV or mental health. Clinicians should follow state law in obtaining approval from the patient to exchange those classes of information. Some states may prohibit electronic transfer of specific classes of information regardless of patient consent.

7. Patient Education and Care Management. Healthcare clinicians are responsible for the information that they make available to their patients online. Information that is provided to patients through PHRs, automated patient education programs, care management and other online services should come either directly from the healthcare clinician or from a recognized, credible and authoritative source.

8. Emergency Subject Matter. Clinicians should discourage use of online communication to address medical emergencies such as chest pain, shortness of breath, high fever, physical trauma or bleeding during pregnancy. Instruct patients to call the office or go to an emergency department for emergency issues. Physicians should consider including a disclaimer on Web pages and emails reminding patients that emergency subject matter is not appropriate for electronic communication.

9. Medical Records. A permanent record of online communications relevant to the ongoing medical care of the patient should be maintained as part of the patient's medical record, whether that record is paper or electronic. Accurate and thorough documentation is effective risk management.

- Providers and patients should be aware that email and online information, including PHRs and consultations, are not erased from a computer's hard drive when deleted and are discoverable in litigation. Therefore all communicated information should be accurate and professional.

Practice Web Site Considerations

1. Authoritative Information. Healthcare clinicians are responsible for the information they make available to their patients online. Information that is provided on a medical practice Web site or provided to a patient via secure email or other online services should come either directly from the healthcare clinician or from a recognized and credible source.

2. Commercial Information. Web sites and online communications of an advertising, promotional or marketing nature may unrealistically raise patient expectations and subject clinicians to increased liability. Liability risks include implicit guarantees or implied warranty and potential violation of consumer protection laws designed to guard against deceptive business practices. This is particularly true when cosmetic procedures, off-label drug use, and non-FDA approved procedures are promoted.

3. Links to Third Party Web Sites and Other Sources of Information. Clinicians are encouraged to post a disclaimer page between their Web site and a link to any third party Web site/information that advises patients and other visitors that they are leaving the clinician practice Web site and that the clinician and the practice do not assume any responsibility for the content or the privacy of other Web sites linked to the practice Web site.

Social Media Liability Risks

Social media (YouTube, Twitter, Facebook, MySpace, blogs, etc.) are used by physicians for physician-to-physician networking. However, these types of media are not appropriate for physician-patient communications, because they are too informal and lack an atmosphere of professionalism – making it easy to lapse into casual conversation and inadvertently cross the boundary between personal and professional relationships. The following recommendations are made regarding the use of social media:

1. Do not discuss individual patients, dispense medical advice, respond to clinical questions from patients or otherwise "practice medicine" on these sites. These types of media do not use HIPAA-compliant secure networks, and inadvertently disclosing a patient's health information will violate HIPAA.

2. Presume that anything you say or post is in the public domain, and remember that anything typed or e-mailed creates a permanent record that is subject to discovery.

3. Physician office practices should have written confidentiality and communication policies with employees that clearly forbid online disclosure or discussion of patient health information.

Personal Health Records

PHRs introduce potential risks. When clinicians offer a PHR service to their patients, the patients/caregivers should be required to accept a PHR Terms of Service Agreement, either online through the PHR service provided or in writing from the practice, which, at a minimum, should include the following:

1. The PHR service is distinct from the medical record maintained by the physician or healthcare provider. Entries in the PHR do not become part of the medical record unless and until they are formally accepted for inclusion by the clinician. When information is imported from a PHR into the clinician's record, its origin should be documented.

2. It should be made clear to patients that physicians are not responsible for knowing the information contained within a PHR except when they have consulted it in association with a formal office visit or Online Clinical Consultation.

3. Patients are responsible for notifying their healthcare clinician(s) if they have a PHR.

4. The PHR is not a substitute for directly communicating the patient's medical information to his or her physician in a traditional format (in-person, by telephone, etc.). Patients should not assume that their Personal Health Record has ever been seen or reviewed by their clinician(s).

5. It is the patient's responsibility to notify their healthcare provider(s) when new information appears in their PHR – whether they personally update it or it is automatically updated by third parties (health plans and other insurers, pharmacies, laboratories, etc.).

6. The provider should make it clear that the responsibility for the accuracy of the information in the PHR remains with the patient or caregiver as the owner of the record.

7. Developing and maintaining a PHR on a clinician practice Web site requires that patients have a pre-existing relationship with that clinician.

8. Materials and information available through the PHR are for informational purposes only and are not a substitute for professional medical advice.

9. Patients/caregivers should agree that they will contact their clinician if they have any questions about their medical condition or if they need medical help.

10. Patients/caregivers should agree that if they need emergency medical help, they should immediately call 911, their local emergency number, their physician, or go to an emergency department.

11. Patients/caregivers should agree that their User ID and Password are their responsibility to protect from unauthorized access and use by third parties.

Electronic Health Record Liability Risks

The EHR has the potential to advance the practice of good medicine. However, when new technologies are adopted, there are always unanticipated consequences. Real and potential liability risks are beginning to be recognized, and it is important for physicians to become familiar with them.

1. Doctors are responsible for information to which they have reasonable access – and there may be increased access to e-health data from outside the practice that enters the practice EHR or Web site or is accessed from the practice EHR or Web site, i.e. hospital charts, consultants' reports, lab results and radiology reports, community medication histories, etc. If patient injury results from a failure to access or utilize available patient information, the physician may be held liable.

2. e-Prescribing is being rapidly adopted, driven by federal financial incentives, and is currently used by approximately 25% of office practices. It works as follows:

a. Most electronic prescriptions are transmitted via a Surescripts network (they have data on 200 million insureds) to all chain pharmacies, 60% of independent pharmacies and most insurance formularies.

b. Most EHRs have an e-Prescribing module, and e-Prescribing is a required capability under the federal financial incentives for Meaningful Use of EHRs.

c. Standalone e-Prescribing software is also available at no cost from Allscripts and the National e-Prescribing Patient Safety Initiative (NEPSI).

d. Most programs also check for drug interactions, dosage errors, medication allergies and patient-specific medication factors.

e. Office prescription renewal requests can be synchronized with this system and with some Personal Health Records.

f. e-Prescribing encourages patients to fill prescriptions (currently 20% do not), because the prescription is sent to the pharmacy electronically and is ready to be picked up when they arrive.

g. Costs are lowered by flagging generic and "on-formulary" drugs.

However, practices are exposed to community medication histories through e-Prescribing; i.e., Dr A renews a medication, and his e-Prescribing program sends an alert advising him that it could interact with another drug. He has not prescribed that drug – so his office staff will have to contact the patient to identify who has, and then Dr A will have to contact Dr X to "negotiate" which drug will be discontinued or changed. If failure to do so results in patient injury from a drug interaction, the physician may be liable.

3. Many EHRs provide e-Prescribing drug information and Clinical Decision Support, and the government's Meaningful Use requirements mandate minimum functionalities in both of these areas. Clinicians should know the source of the drug and Clinical Decision Support information in their EHRs, because the standards to which they may be held accountable are the clinical standards for their specialty and the information in FDA-approved drug labels or drug Alerts.

4. Doctors may ignore, override or disable alerts, warnings, reminders and embedded practice guidelines – due to "alert fatigue." If it can be shown that following an alert or guideline would have prevented an adverse patient event, the physician may be found liable for failing to follow it.

5. Meaningful Use requires online patient connectivity, and many EHRs have patient questionnaires that utilize an algorithm to interview the patient. These questionnaires often address, and memorialize in the record, issues that many physicians are simply not prepared to pursue (depression, substance abuse, etc.). Lack of or incomplete follow-up can create potential liability – and there is a clear record for the plaintiff's attorney to follow.

6. Vendor contracts may attempt to shift medical liability risks resulting from faulty software design or decision support data onto the physician. They may also provide that the vendor has rights to utilize patient or provider data. Read these contracts carefully.

7. Electronic Discovery: Lawyers may request not only printed copies of the EHR but also the "raw" e-data for metadata analysis, i.e. log-on time, what was reviewed and for how long, what changes or additions were made – and when, log-off time, etc. Smart phone and email records are also discoverable. Physicians need to know that all of their interactions with the EHR are time-tracked and discoverable.

8. Doctors may "copy" information from a prior note or visit and "paste" it into a new note or visit (known as "cloning"), making changes where appropriate or documenting by exception. This may result in irrelevant over-documentation and the patient may appear to have more or less complex problems since the prior encounter. By substituting a word processor for the physician's thoughtful review and analysis, the narrative documentation of daily events and the patient's progress may be lost, thereby compromising the record of the patient's course. The quality of notes and documentation may be further compromised by the use of templates.

9. EHRs may auto-populate fields in the History and Physical (from data derived from data fields in a prior H&P) and in Procedure Notes (from personalized or packaged templates). While over-documentation may facilitate billing, if erroneous or outdated information is entered, it may increase liability. For example: An internist was deposed and his EHR was the medical record. Some of the auto-populated fields contained obviously wrong information, and at deposition the plaintiff's attorney asked these questions:

a. "So is the information in this record accurate or not?"

b. "Do you bother looking at your records?"

c. "If these 'auto-populated' fields are incorrect, can we trust anything in this record?"

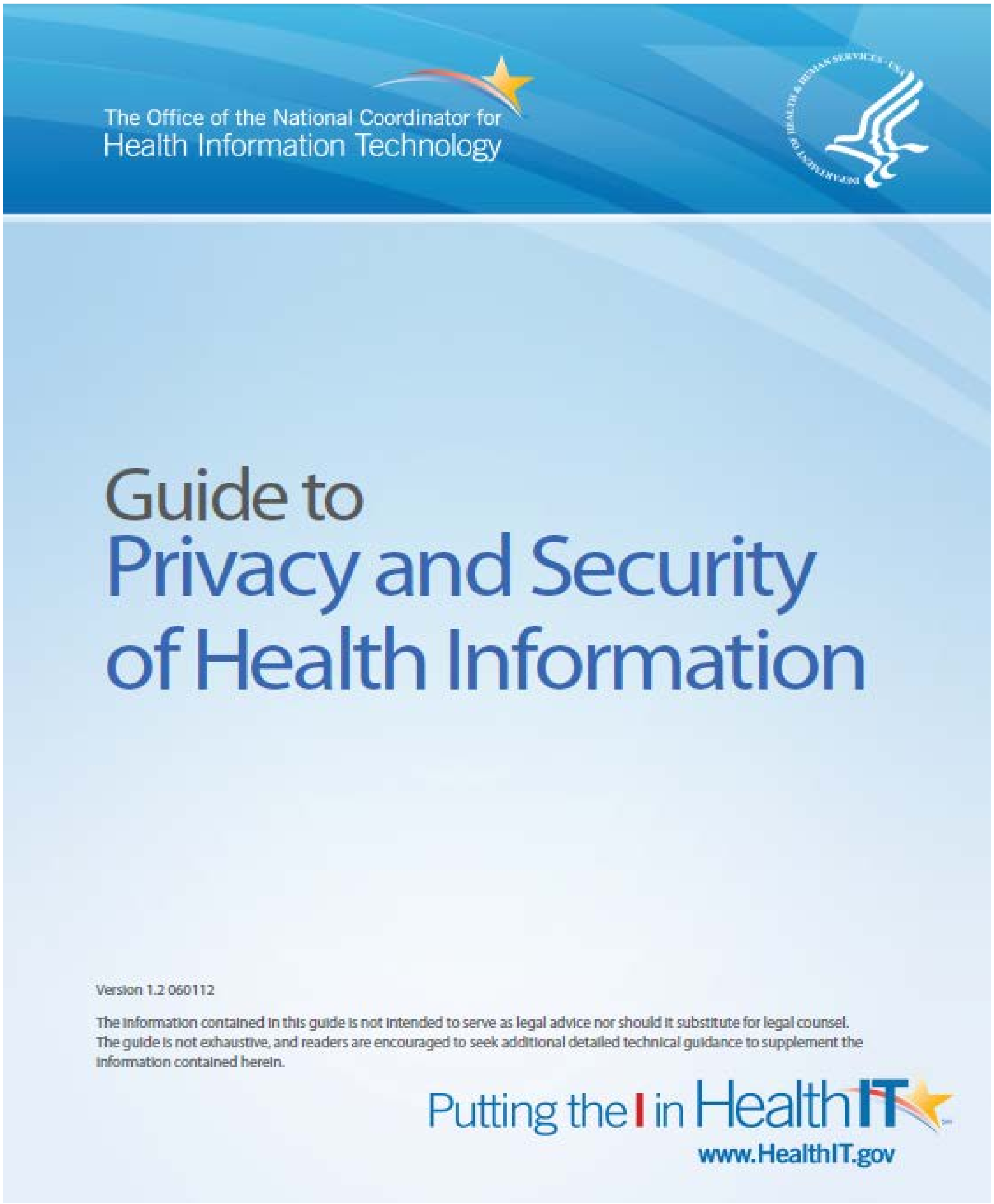
d. "Do you deliver the same level of care as you do in record keeping?"

Templates with drop down menus facilitate data entry. However, they are usually integrated with other automated features, and an entry error may be perpetuated elsewhere in the EHR – and overlooked, resulting in a new potential for error. Erroneous information, once entered into the EHR, is easily perpetuated and disseminated.

10. The computer may become a barrier between the doctor and patient – as the doctor fills-in a computer template that diverts attention from the patient and restricts creative thinking. This may weaken the doctor-patient relationship.

GUIDE TO PRIVACY AND SECURITY OF HEALTH INFORMATION

http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf



The Office of the National Coordinator for
Health Information Technology

Guide to Privacy and Security of Health Information

Version 1.2 060112

The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

Putting the I in Health IT

www.HealthIT.gov

Guide to Privacy and Security of Health Information

The Office of the National Coordinator for Health Information Technology

Contents

Contents

Guide to Privacy and Security of Health Information

The Office of the National Coordinator for
Health Information Technology

As with any new program or regulation, there may be misinformation making the rounds. The following table distinguishes fact from fiction.

Security Risk Analysis Myths and Facts

Myth	Fact
The security risk analysis is optional for small providers.	**False.** All providers who are "covered entities" under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.
Simply installing a certified EHR fulfills the security risk analysis MU requirement.	**False.** Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.
My EHR vendor took care of everything I need to do about privacy and security.	**False.** Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.
I have to outsource the security risk analysis.	**False.** It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.
A checklist will suffice for the risk analysis requirement.	**False.** Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.
There is a specific risk analysis method that I must follow.	**False.** A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guidance assists organizations in identifying and implementing the most effective and appropriate safeguards to secure e-PHI.
My security risk analysis only needs to look at my EHR.	**False.** Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data. Please see U.S. Department of Health and Human Services (HHS) guidance on remote use.
I only need to do a risk analysis once.	**False.** To comply with HIPAA, you must continue to review, correct or modify, and update security protections. For more on reassessing your security practices, please see the Reassessing Your Security Practice in a Health IT Environment.
Before I attest for an EHR incentive program, I must fully mitigate all risks.	**False.** The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) during the reporting period, as part of its risk management process.
Each year, I'll have to completely redo my security risk analysis.	**False.** Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior analysis for changes in risks. Under the Meaningful Use Programs, reviews are required for each EHR reporting period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP's year of participation in the program.

To learn more, visit the Privacy and Security Resources page for more information.