EMRapproved.com

Will your HIPAA Risk Analysis Pass a Meaningful Use Audit or Data Breach Investigation?

SEMEL CONSULTING

Q: How does a provider know if their Email system has encryption? Do big email services (gmail, yahoo, hotmail, etc.) have built-in encryption?

A. Most e-mail systems do not include encryption. There are add-on solutions and services that include e-mail encryption. Several companies offer encryption tools that can look at the message and certain attachments and-- by rule setting like identifying health information or things like Social Security numbers-- automatically encrypt a message. These also allow you to manually encrypt a message. Within EHR systems, the mail remains secure because the users have to log into the system

Q: Will passwords that meet specific requirements mitigate fines if laptops with records are stolen?

A. Passwords themselves will not mitigate fines. The data stored on laptops and other devices is known as 'data at rest.' This data must be encrypted using a specific program or hardware device that makes the data unreadable in accordance with federal standards. The National Institute of Standards & Technology (NIST) has issued a special publication 800-111 which

Q: are you a CISSP?

A. No, I focus more on compliance than technical security. I am a Certified Business Continuity Professional; Certified HIPAA Professional; Certified HIPAA Administrator; Certified Security Compliance Specialist; and Certified HIT Specialist. I was a hospital CIO and have owned or managed technology firms for over 30 years.

Q: HIPAA guidance, prior to meaningful use, recommended a risk analysis at least every three years.

A. The HIPAA guidance for risk analysis has changed over the years. Recently the State of Alaska Department of Health and Social Services was fined for a data breach, and one of the findings was that their risk analysis was not current. In an interview, their CSO said that he took issue with that finding because there was no clear guidance on the frequency of a risk analysis. Meaningful Use requirements are that the risk analysis be conducted or reviewed each year to determine any vulnerabilities that should be mitigated. There is also guidance that says that if anything 'significant' changes your risk analysis should be updated as needed.

Q: Regarding MU audits, reporting anomalies do appear to be one trigger - i.e. if multiple measures have a denominator of unique patients seen by the eligible professional within the reporting period and one of the measures has a significantly different denominator than other similar measures.

A. It makes sense that reporting anomalies would trigger an audit. Today an online article said that some EMR companies are reporting health care organizations who claim to use their software but have not purchased licenses.

Q: Security awareness education needs to be provided to all workforce members who have access to ePHI which may include students, interns, etc. that are not paid employees.

A. Security awareness (reminders) and training are required of all workforce members as you described. The new

Q: Are there slides for the presentation?

Yes, these are published at www.emrapproved.com.

Q: Is the covered entity responsible for training their business associates?

A. No, a Covered Entity is not responsible for training their BA's. However, my opinion is that the Covered Entity should be comfortable that their BA's have implemented an internal compliance program-- including training-- to be sure that the BA does not cause a data breach.

Q: Are there regulations that specify who should conduct employee training on HIPAA and policies and procedures?

A. There are no regulations regarding who should conduct training. In some situations organizations hold group classes, others use electronic learning management systems to deploy and track training. Whatever you choose, make sure your

Q: Do suggest any additions to the typical security risk analysis based on the new EHR certification criteria that will take effect in 2014 based on the new 2014 edition certification criteria?

A. There is a new guideline for encryption and the removel of protected data if an EHR system is no longer being used. The risk analysis should ask specific questions about validating encryption or else the risks could be either/or a data breach or compliance violation.

Q: What was the name of the federal office again?

A. The Office for Civil Rights in the US Department of Health and Human Services is responsible for enforcing the HIPAA

Q: but what about blackberries for example. you have to depend on passwords. you cant encrypt it. because you couldnt read it?

A. Encryption is not a mandate, but if a device is lost and it is encrypted, you do not have to report the loss. If you use a device that cannot be encrypted, you have to decide if the risk of a reportable data breach (and the associated costs, which can be huge) is worth it compared to the convenience of having the data on the local device. There are now apps for smart phones that allow to access protected data from a remote server. The data never transfers to the local device, so while you need to be careful about someone seeing the data on your device, you do not have to worry about encryption.?

Q: how would you know if the email response coming back to you is encrypted or not?

A. An encrypted e-mail message points you to a site where the original is stored in an encrypted system. You have to

Q: Can a BA be assessed penalties for noncompliance, or would this be rolled up to the CE they provide services for?

A. The HITECH Act included a provision that BA's will have to comply with HIPAA and face penalties similar to Covered Entities. In a recent interview, Leon Rodriguez, the Director of the Office for Civil Rights, and a former prosecutor, said that after OCR publishes the new rules (expected this year) that BA's will be given 180 days to comply before enforcement begins. Remember that your BA Agreement can contain language that requires BA's to pay the costs associated to a breach that they cause. So, until OCR begins enforcing compliance on BA's, you can enforce financial responsibilities through your contracts. And a Covered Entity may also be penalized for not ensuring that their BA's are compliant.

Q: If Business Associates can be penalized directly, do you know if that happened in the recent example of the hospice in Idaho?

A. The BA in Idaho lost the business from the hospice, but was not penalized by OCR because the agency rules have not yet been implemented (see above.)

Q: What sort of fines can be assessed to managers in an organization as a result of an audit or breach where the individual was not blatently violating the regulation, yet a breach occurred due to other reasons? At what level could that happen?

A.There have been several publicized incidents where hospital employees have been fired for snooping in patient records of celebrities and family members. I do not know of any situation where an individual manager was fined for a breach; the civil penalties are against the covered entities they work for. Criminal HIPAA penalties are prosecuted through the US Department

Q: is there a standard bussiness associate agreement letter or form that we can use?

A: EMRapproved has a template available on its website. As with any legal document, before using it you should have it reviewed by a competent attorney familiar with your situation and needs.

Q: Please clarify the risk analysis mitigation...if a facility has a work plan in place to mitigate the risks they were unable to complete at the end of the attestation period due to the size of the organization or the complexity of the risk, is this acceptable as long as there are specific dates the risk areas have to be mitigated?

A: The Office of the National Coordinator Guide to Privacy and Security of Health Information states that 'The EHR incentive program requires addressing any deficiencies identified during the risk analysis during the reporting period.' This seems clear that the mitigation must take place during the reporting period, but we have not seen evidence of how this is being enforced. After several of the data breaches the parties being penalized stated that they had started compliance programs but had not finished them. The State of Alaska DHSS CSO said that he had started encrypting devices but had not gotten to the portable hard drive that was lost and cost his agency a $ 1.7 million penalty. This indicates that results outweigh plans and schedules.

Q: where is the Risk Analysis myths and facts document located?

A. The Myths & Facts are located on www.emrapproved.com.

Q: Would you say in a nut shell all systems pertaining to ehr/emr should be free of compromise regarding patients sensitive or your likely to be audited or fined for a breach of information?

A: It is a fact that patient data must reside on a system. The system should be secured using HIPAA Security Rule Administrative, Physical, and Technical safeguards. Audits have been done by random selection, and most breaches have occurred because of a failure to implement Administrative, Physical, and Technical safeguards. Breaches can be reported through official reporting mechanisms or by whistleblowers. Lost portable devices would not be the cause of data breaches if (a) Administrative policies against transporting data were in place and enforced (b) if the devices had been secured against theft using Physical protection and (c) if encryption had been implemented (a Technical safeguard.)

Q: How can an organization deal with security when using text messaging on smart phone?

A: Standard text messaging is not a secure method of communications and should not be used to send ANY protected information. Period. Just look at the scandals with the British press who easily hacked into text message systems. When you 'delete' a message it stays on the carrier's system, which is often brought up on news reports about a text message that is used in a criminal investigation or trial. There are secure text messaging system for health care providers. One other way to prevent a breach is to reference, say, a patient's name and phone number but nothing describing a treatment or diagnosis.

Q: If a patient provides the office the name of a physician as referring physician or PCP and they do not update it on future visits even though requested to do so, is it a breach if a summary of the office visit is sent to one of the original providers even though the patient no longer will be seeing that provider?

Q: Can you give us a web site for NIST?

A: http://csrc.nist.gov/publications/index.html

Q: If patient info is sent via encrypted email to an outside entity (ie: Collection Agency), are we liable to ensure that the outside entity's email is encrypted when they respond, or is this solely their responsbility?

A: A Collection Agency is your Business Associate so if they breach the data you sent them-- in any way -- you are the responsible covered entity and subject to penalties. Sending unencrypted e-mail creates risk because a message can be read if intercepted, thus creating the risk of a breach. Unless you have a Business Associate Agreement with them (it surprises me how many Covered Entities work with partners but do not have them sign BA's) then your sending them the original message and allowing them to see your patient data may be a breach itself.

Q: Is there a complete definition of the E.H.R. "system," since many large organizations have multiple modules that comprise parts of the medical record...including RIS/RAD, Pharmacy, Lab and other systems. Do these have to be included in the risk assessment process, or is it enough to include the patient record systems themselves, since the data mostly gets passed to that system?

A: All devices that store or transmit Electronic Protected Health Information (ePHI) must be included in the Risk Analyis. When we discuss an EHR system we are most often referring to a certified system that quailfies for the federal EHR Incentive Program. Health care organizations are often surprised to find the many places that ePHI can hide, including hard drives in

Q: If my company secures a letter from a business partner, stating they assume the breach risk for sharing PHI data with an insurance broker, free me of breach responsibility?

A: Without knowing specifically about your relationships and responsibilities, I cannot tell if you are referring to a Covered Entity or Business Associate. Currently a Covered Entity (a payer, or insurer) is responsible for a data breach, and must have their Business Associates sign agreements. In the agreement the responsibilities of each party can be defined. No letter can absolve someone of their responsibility to comply with the law, so you should consult with an attorney to determine what best fits your situation.

Q: I work for a Regional Extension Center and we are looking at providing SRA's as a means of sustainability. What liability concerns might there be with proving an SRA?

A: As with any type of document (including sample legal agreements,) you can state a limit of liability on the document or in a contract with your clients. Liability advice is best provided by an attorney.

Q: So do we need to have BA agreements with all pharmacy's that we send electronic, faxed or verbal prescriptions to?

A: No, pharmacies are Covered Entities and Covered Entities do not need Business Associate Agreements to share patient info for treatment, payments, or health care operations.

Q: Does that include patients for whom you are both the attending and consulting physician? or just attending?

A: Physicians are Covered Entities and can share patient data regarding treatment without needing a BA Agreement.

Q: What is the link to the audit criteria that you mentioned?

A: The audit criteria is available at www.emrapproved.com.

Q: I work for an EMR vendor. We instruct our clients to set up security (which has a feature for emergency access), encrypt their database, manage audit logs, encrypt all docs in the EMR, and validate that no one has tampered with a file. Will this suffice? Now...we also tell clients that since our EMR is certified by the ONC, they don't need to follow all those security features - it's good enough that the EMR has those capabilities. Is that okay for stage 1?

A: I am a bit confused about the wording of your second question, particularly about telling clients they don't need to follow your security features. Within your system you have features that protect the data against data breaches. Most practices have protected data on devices (servers, desktop and laptop computers, portable drives) outside of EMR systems, and that data must be protected as well as what is in your system. Feel free to contact us through the EMRapproved website to clarify your

Q: What are some of the audit protocols that are being missed during the risk analysis process?

A: I find that during a risk analysis I often have to interpret questions, and give some examples, because there is often some misunderstanding or confusion with the question as written. Sometimes we have to ask questions of a non-technical practice manager who will then refer us to IT for some answers. Things often missed are clearly written policies that comply with HIPAA; adequate documentation of procedures used to comply with the policies; and having evidence that prove you actually do what your polocies and procedures define.

Q: Are the risk vulerabilities required to be physically verified during the RA process OR is the interview process with IT sufficient to document for the RA.?

A: There is no requirement for physical verification, however, I think it is a good idea to verify at least a sample of security

Q: How different is Core Measure #15 from FDA’s 21 CFR Part 11 for ensuring data integrity in terms of electronic records and signatures?

A: It depends on how you define 'different.' While many of the goals and requirements are similar, Core Measure 15 specifically references 45 CFR 164.308(a)(1) (the HIPAA Security Rule) and is part of the EHR Incentive Program. If your question is "If we comply with FDA 21 CFR Part 11 do we comply with Core Measure 15?" I would suggest you create your risk analysis to comply with HIPAA and not hope that your FDA documentation will stand up to the scrutiny of an EHR audit with

Q: Any suggestions about resources (consultants) that offer services for risk/security analysis for a small practice, and likewise for a practice group?

A: Semel Consulting offers these services through EMRapproved.

Q: The comment about breaches doesn't seem to comply with applicable regulations which indicated that before there is a breach, there must be a significant risk of harm to the patient.

Reply: The HIPAA data breach laws state that a breach must pose a significant risk. When the Massachusetts Eye and Ear Infirmary had a doctor's laptop stolen in Korea, and they remotely wiped it clean, then determined that there was no harm to any patients, they paid a $ 1.5 million penalty. When medical billing records were discovered at a trash facility, a state attorney general stated that the patients were "at risk" and levied a $ 140,000 penalty even though no harm was proved. The use of an Internet-based e-mail system was considered the basis for a $ 100,000 penalty to a Phoenix area medical practice because they 'impermissibly disclosed electronic protected health information (ePHI) by making it publicly available on the Internet' even no harm was proved. These actual penalties indicate that the threshhold for "significant risk" varies widely. Also, there are 46 states with their own data breach laws.

Q: That isn't correct. It isn't a data breach unless the security breach causes a breach of the privacy rule so if the unsecured email was not a privacy breach there is no duty to report a breach.

Reply: Simply sending a message through an unsecured e-mail system is not a breach by itself, but drastically increases the risk of a breach. Again, just the use of an Internet-based e-mail system was considered the basis for a $ 100,000 penalty to a Phoenix area medical practice because they 'impermissibly disclosed electronic protected health information (ePHI) by making

Q: What typre(s) of incidents are required to be reported? Are there a specific # of patient files that need to be involved?
A: The HIPAA data breach laws are described at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html. There are varying requirements depending on the number of patient records and also state regulations.

Q: Is a unauthorized disclosure that doesn't cause any financial, reputational, or other harm a breach?

A: The Breach Notification rule states "A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual." Forty-six states have data breach laws-- some require proof of harm and others require that all unauthorized releases be considered breaches. As mentioned above, the unauthorized release of patient data has resulted in very large penalties even though those penalized claimed that no harm was done.

Q: My experience with many medical offices is that they're more concerned with privacy of patient of information, but have little understanding of IT security. That was confirmed with the publishing of an article in the Washington Post recently http://www.washingtonpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html?

A: Our experience is similar. It was easy to implement Privacy Rule compliance compared to the ever-changing IT enviroment with its multitude of threats and vulnerabilities. I thought the Post article was enlightening and frightening to some who just expect their most personal information to be better protected.

Q: Our Radiologistw work within a health system. Altough the physicians have purchased their own EHR it is "fed" patient information from IT sources that are controlled by the health system. Since the physicians do not have control over the health system risk management testing how can they adress this with regards to MU requirements?

A: I have specific experience with a HIPAA audit for a radiology practice where we had to evaluate the practice's billing office environment and IT systems, as well as systems located in hospitals across the region. We coordinated our effort with the hospital IT staffs to get a total picture of the IT environments. Everyone cooperated and this approach was sufficient for HIPAA and I think logically extends to Meaningful Use.

Q: How does the audit apply if during the reporting period of implementing a new EMR system and all HIPAA requirements where being set up, tested and implemented, staff education, etc.but the physical document is yet to be developed to outline all that has been put in place? Is it a problem to continue the "completion" of the document itself before the Feb. attestation deadline? Other words it was done but the phyiscal documents are not to satisfaction yet.

A: The requirement is for the Risk Analysis and the mitigation to take place prior to the end of the reporting period (the last one for 2012 ended 12/31/2012.) There is nothing I have seen specific to the documentation date, but logically it makes sense to have a report done prior to attestation (deadline is 2/28/2013) so there is auditable evidence that the risk analysis and mitigation took place.

Q: A practice decided not to give patients their clinical summaries because the clinical summary may end up littering the parking lot and could be a HIPAA violation. Would this be a violation or not?

A: Once the practice provides a patient any protected data the patient can do whatever they want with it. If the patient loses the information in the parking lot it would be a mess but not a breach caused by the practice. However, it may be very hard to prove that patient data blowing around the neighborhood was caused by patients and not the practice. Large fines have been levied because protected data ended up in the trash.

Q: does the risk analysis have to be done before end of the reporting period for MU? if I am in 90 day and my end of 90 day is 11/1/2012, it must be done before 11/1/2012, right?

A: Yes and Yes. The Office of the National Coordinator Guide to Privacy and Security of Health Information states that 'The EHR incentive program requires addressing any deficiencies identified during the risk analysis during the reporting period.'

Q: Is there a good risk assessment template that we can use? There seems to be many out there, but which one can help us pass our audit?

A: The Office of the National Coordinator has templates you can use. You need to determine what best helps you identifies threats, vulnerabilities, impact, and liklihood, and leads you to solutions that can help you mitigate the risks during the reporting period. Guidance is available at **http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.** One of the Myths and Facts asks if you must use a consultant to conduct a risk analysis. The answer is no, but then the ONC offers this comment: ' ...doing

Q: If our internal email (Outlook) is not encrypted, but is sent through our secure network , is that okay? We use Cyglan for external email.

A: Yes, as long as you have policies, procedures, and technical tools in place to ensure that only your authorized workforce members can access your system.

Q: Will the EHR vendor ever fall in the scope of an audit and in case if any breach is found will the EHR vendor be responsible in addition to the health care provider.

A: An EHR vendor is a Business Associate, and BA's will have to comply with HIPAA based on the HITECH Act. Since Covered Entities are now subject to audits it seems logical that BA's will also be. If you breach a health care provider's protected information you may be responsible now based on your Business Associate Agreement, and will be independently responsible when BA enforcement begins.