The HIPAA Security Risk Analysis

By
Dr. Ron Short, DC, MCS-P, CPC

ICD-10 "Grace" Period

- On Monday, July 6, CMS announced that they will allow some latitude with the ICD-10 codes.
- For one year after the implementation of the ICD-10 on October 1, CMS will reimburse for wrongly coded claims as long as the erroneous codes are in the same broad family as the correct codes.
- Also, the coding error has to be the only error on the claim.
- This will serve as a transition for the ICD-10 and allow doctors and staff to become proficient with less potential income loss.
- An example of this might be using M25.531, pain in the right wrist instead of M25.532, pain in the left wrist.
- You will still need to be proficient and accurate with ICD-10 by October 1, 2016, but you will have some time.

EHR Stage 2 Reporting

- Information is going around that there are changes in reporting requirements for Stage 2 EHR.
- At this time, there are proposed rule changes.
- They have not yet been finalized.
- It is expected that the final rule will be published in August or September of this year.

HIPAA Security Risk Analysis

- From the 2015 OIG Work Plan:
- We will perform audits of various covered entities receiving EHR incentive payments from CMS and their business associates to determine whether they adequately protect electronic health information created or maintained by certified EHR technology.
- In short, they will look to see if you have a properly done your Security risk Analysis.
- According to CMS guidance issued November 5 2014, the Security Risk Analysis (SRA) may be completed at any time after the start of the reporting year and before the provider's attestation date.
- Measure 9 of Stage 2 meaningful use states:
- Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a) (1), including addressing the encryption/security of data stored in CEHRT in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process for EPs.
- 45 CFR 164.308 (a)(1) states: Implement policies and procedures to prevent, detect, contain, and correct security violations.
- This includes;
    - Administrative safeguards
    - Physical safeguards

- Technical safeguards

10 Myths about the SRA

- 1 – A Security Risk Analysis is optional for small providers
  - If you are a HIPAA covered entity a Security Risk Analysis is mandatory
  - If you are pursuing a HER incentive by way of meaningful use attestation a Security Risk Analysis is mandatory
  - Research indicates that about 30% of all data breaches occur in organizations with 100 employees or less
- 2 – Any certified EHR system will satisfy the Security Risk Analysis requirements
  - The Security Risk Analysis covers all PHI, not just that in your EHR. This goes far beyond your computer files.
  - Many offices still maintain some form of paper files.
  - Most doctors are now using tablets and smartphones in addition to their office computers
- 3 – EHR venders already address privacy and security issues for their customers.
  - Many times EHR venders will offer information about security but this information is not usually specific to your office.
  - Each office is unique and requires unique solutions.
- 4 – There is a single method of analysis that must be followed.
  - Each practice is unique and the threats to PHI are unique as well.
  - The Office of Civil Rights guidance recommends that effective analysis includes;
    - Identification of PHI data sources.
    - Identification of human, digital, and environmental threats to that data.
    - Assessment of current security measures.
- 5 – Checklists will satisfy the security risk analysis requirements.
  - Checklists are a nice reminder but they do nothing for implementation.
  - A good Security Risk Analysis includes action steps to mitigate the risks identified.
- 6 – A Security Risk Analysis only needs to be completed once.
  - A good SRA identifies deficiencies and lists corrections.
  - As you take the corrective action you should document what is done and when.
  - You should then re-assess your security at least annually.
- 7 – Each new Security Risk Analysis needs to start from scratch.
  - When done properly the initial SRA will serve as a framework for future re-evaluations and updates.
  - Each action step that is taken needs to be documented.
- 8 – I have to hire someone to do the Security Risk Analysis for me.
  - This is not always the case.
  - There are tools available to you to assist you in the development of a SRA.
- 9 – The Security Risk Analysis covers my EHR only.
  - There is more that needs protected than just your HER.

    - The SRA should cover:
        - Your facility.
        - Your hardware.
        - You software.
        - Your staff.
        - Your documented policies.
- 10 - I have to completely redo the Security Risk Analysis each year.
    - If you do not do it right the first time, you may have to.
    - However, when you do it right it serves as a foundation for all future security assessments.
- These myths are what keep doctors from producing appropriate SRAs.
- The SRA is like your office compliance program, it is an ongoing program that you periodically update.
- It is not another government mandated notebook that you set on your shelf and forget.

HIPAA Security Risk Analysis

- There are 10 elements to a SRA
    - 1 - Inventory Assets
    - 2 - Determine where ePHI is stored, processed or transmitted
    - 3 - Set the scope
    - 4 - Identify and document threats
    - 5 - Identify and document vulnerabilities
    - 6 - Determine current security measures in place
    - 7 - Determine and prioritize risks
    - 8 - Assign responsibilities and target dates
    - 9 - Finalize documentation
    - 10 - Periodically review
- This will lead you to develop a documented security plan that addresses the confidentiality, integrity and availability of ePHI and will include strategies for:
- Continuity plan
- Emergency access plan
- Disaster recovery plan
- Vendor management plan
- The completion of the SRA and the development of your security plan will cause you to think about things that you may not have considered before.
- There are many details to cover and questions to be answered.
- Fortunately, CMS has a tool to help you with this.
- You can find it at; http://www.healthit.gov/providers-professionals/security-risk-assessment
- They also have a user's guide to help you.
- You can find it at; http://www.healthit.gov/providers-professionals/security-risk-assessment-videos
- When you go to the website, you will want to download the tool to your computer.

- When you first open the SRA Tool, you will put in your first and last names and initials in the appropriate area.
- You can also put in information about your practice.
- You would next list those business associates that would have access to PHI (both electronic and physical).
- Lastly you would inventory your assets.
- Then you will log in to the tool.
- When you log in you will see an informational page with examples of administrative safeguards, physical safeguards, and technical safeguards.
- From here you will start the assessment by clicking on the "start assessment" button.
- You will be presented with a series of yes and no questions one at a time.
- The questions will be in one of three categories; standard, required, or addressable.
    - Standard – this is evident in the specification and is used to develop a security policy.
    - Required – Failure to include this specification is an automatic failure to comply with the HIPAA security rule.
    - Addressable - The covered entity must assess and decide whether it is a reasonable and appropriate safeguard in the entity's environment and if so the entity must implement, or
        - Implement an equivalent alternative measure
        - Document the reason for not implementing
        - Addressable does not mean optional
- You will also have three tabs in the right hand column that will give you related information regarding the question. They include;
    - Things to consider
    - Threats and vulnerabilities
    - Examples of safeguards
- There are tabs at the bottom that let you access;
    - The report
    - The glossary
    - The navigator
    - The related information tabs
- You navigate through the questions by using the "next question" and "previous question" buttons.
- When you answer a question the tool will pop up a new window where you can list your current activities regarding this question.
- You will also be asked to assess the likelihood and impact of this threat affecting your ePHI.
- If you answer no to the question you will be asked to give the reason why it is no.
- You should then make complying part of the remediation plan.
- As you complete the questions you will generate a report.
- You will do this for the 156 questions in the tool.
- You now have a report. You must be done.
- Not quite.

- Now that you have identified the risks and what you are doing about them, you need to do two more things;
- Make a plan to correct the deficiencies and conduct follow-up reviews, and
- Write policies and procedures to implement the plan.
- Failure to complete these steps means that you do not have a complete Security Risk Analysis.
- Now that you have identified the deficiencies in the analysis report you need to develop a plan to correct those deficiencies.
- The plan should include action steps and a deadline for each deficiency corrected.
- The important point is to document that you are taking definitive steps to correct the deficiencies.
- Once you have a plan to correct the deficiencies you need to develop security policies for you office.
- Fortunately CMS has provided a template for that.
- You can find it at; http://www.healthit.gov/node/289.
- The template is in Word format and is 94 pages long.
- Some policies may not apply to your practice and can be deleted.
- The Security Risk Analysis, the Mitigation Plan, and the Security Policies should be incorporated as a section of your HIPAA manual.
- All of this is part of HIPAA compliance as well as part of attestation for meaningful use.

Summary

- It is very important for you to consider the threats to the privacy and security of your practice and take appropriate corrective action.
- The responsibility for the protection of patient records belongs to the doctor.
- The fines for failing to do this can be severe.

Downloadables

- The Security Risk Analysis Tool:
  - http://www.healthit.gov/providers-professionals/security-risk-assessment
- The SRA Tool User's Guide:
  - http://www.healthit.gov/providers-professionals/security-risk-assessment-videos
- The Security Policy Template:
  - http://www.healthit.gov/node/289