OCR HIPAA Security Audit Protocol – a second look


OCR states on this web page:

“The OCR HIPAA Audit program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits. The entire audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. The combination of these multiple requirements may vary based on the type of covered entity selected for review.

The Security Audit Protocol covers the Security Rule requirements for administrative, physical, and technical safeguards. This Protocol has 77 entries outlined against many but not all of the HIPAA Security standards and implementation specifications.

The OCR Security Audit Protocol has 5 headings that are not explained or defined.

The **Section** is the Code of Federal Regulations (CFR) section for the specific HIPAA standard for the next 4 columns.

The **Established Performance Criteria** either is the CFR language or an explanation of what is expected per audit protocol.

The **Key Activity** column outlines what you must be doing such as developing awareness training, content, materials, and methods, or the process steps relating to the overall objective.

The **Audit Procedures** are what the auditor is going to ask you for to prove compliance and implementation. For example, you will be asked for management interviews about your organizations’ HIPAA compliance program, policies, procedures, plans, job descriptions and many other things.
The Implementation Specification only notes required [R] or addressable [A].

**What is an OCR Security Audit?**

An audit is a formal or official examination and verification of an organization’s HIPAA Security compliance and implementation.

It is an accounting, scrutiny, and inspection or a review. It should not lead to an investigation unless the audit finds a gaping hole in your HIPAA Security controls and implementation.

During the first round of audits in 2011 OCR discovered that one entity had not done a Risk Analysis. Something like this found in your organization will provoke an OCR investigation with all its bells and whistles.

**HIPAA Security Audit Protocol Review**

In my in-depth review with the MalvernGroup of the OCR HIPAA Security Protocols we discovered a number of issues that I want to bring to your attention.

1. The protocols are asking both Code of Federal Regulation (CFR) questions and practical questions. They are asking both these type of questions as you are going to need to prove that you comply with the all the necessary regulation sections for your type of entity and provide evidence of implementation of the regulation sections.

   For example, for security section 164.308(a)(8), Evaluation, you are asked both if you have conducted an evaluation and what type of documentation you have for your evaluation, such as standards and measurements used for evaluation, and findings of an evaluation.
2. As with anything new we must learn a new language. The Security Audit Protocol uses about every term in the book for individual employee, but workforce, including staff, contractors, vendor and others.

3. A whole new set of terms and concepts not found in the HIPAA regulations, such as informal policies and procedures. I wonder what INFORMAL policies and procedures are!

Are both formal and informal policies and procedures written documents? Or are they informal in understanding? Are they casual? Irregular? Unofficial? Unconventional? Perhaps OCR will clarify if enough of the individuals and entities being audited in this round do not understand what informal means.

I recommend that all your policies, procedures and plans be in writing, be in your policies and procedures manual, and be part of your training plan.

4. The run of the criteria and audit procedures are not always in the order of the security rule.

Plus, the not all sections and requirements of the HIPAA Security Rule are addressed in this first version of the Security Audit Protocol.

5. Sometimes the compliance questions are asked first and then the practical questions and at other times it is the opposite. There does not appear to be any rhyme or reason for this that I have yet discovered.

This makes it difficult to determine how to prepare and what you need to have ready for an OCR audit.

6. In the security 164.310(b), Workstation use, section two key activities (Identify workstation types and functions or uses, and Identify expected performance of each
type of workstation) have identical audit procedures, which is not useful as one activity is a listing of types, functions and uses, and the other is a performance question.

7. Several of the key activities or audit procedures ask for work that may appear to be neither CFR compliance, nor evidence of implementation. You may want to consult your attorney or compliance office to help you interpret these areas.

8. Several of the Security audit procedures outlined appear to be reaching beyond the Security Rule requirements. You may want to consult your attorney or compliance office to help you interpret these areas.

9. There is the expectation that screen shots will be submitted as implementation evidence.

During our in-depth review of the OCR Security Audit Protocol I had this thought running around in my head – the drafters of the protocol were good auditors, but did not have quite a full grasp of the HIPAA Security requirements.

In an attempt to help you understand and collect all the information you will need in one tool, in one place, the MalvernGroup has created an OCR HIPAA Security Audit Protocol workbook in table format by adding 5 more columns to the 5 within the OCR Audit Protocol tables. The new columns are:

**Requested Evidence**

The Requested Evidence column is derived from interpreting the Established Performance Criteria, Key Activity and Audit Procedures columns. It represents what MalvernGroup thinks the auditors would request in order to perform their audit procedures as they are carried out.
Availability

You may use this column to document where you stand in relation to the Requested Evidence column.

Document ID

You may use the Notes column to unambiguously identify the evidentiary document.

Document Owner

The Document Owner column can be used to document who or the role that is responsible for the document.

Document Location

You may use the Location column to document which information system houses the document or the location of any paper documents.

MalvernGroup has attempted to decode each Security Audit Protocol row and entered suggested documents and other evidence in the Requested Evidence column. This is to help you begin the discussion within your organization. You can add and delete in the Requested Evidence column to match you structure and services.

MalvernGroup has also annotated the 77 rows of the MS Word table with more than 50 footnotes and includes a table of contents for easy access to the Key Activities, as defined by the OCR HIPAA Audit Protocol. Among the footnotes are the areas the MalvernGroup suggests that may be beyond the Security Rule standards and implementation specifications.
You will find the Malvern Group OCR HIPAA Security Audit Protocol Workbook at http://www.malverngroup.com/Publications.html. MalvernGroup plans a webinar on the OCR HIPAA Security Audit Protocol Workbook in August. We will announce the webinar on our website and in the weekly alerts we send out. You may sign up for the alerts at http://www.malverngroup.com on the bottom of the page.

MalvernGroup is also creating a workbook for the HIPAA Privacy and Breach Audit Protocol. We will announce on the website when the second OCR Audit Protocol workbook is available.

**Conclusion**

Each type of covered entity and business associate can now plan their own audit using the information on the OCR website, the MalvernGroup workbook or one you develop yourself.

Any entity that has used the NIST HIPAA Security toolkit, using either version, will have many of the answers they need for the OCR HIPAA security protocol to demonstrate compliance with the section and have documented evidence of implementation as well.