A-Z Audit/Evaluation

Annual Compliance Program and Security Rules

This is an ***audit*** *of your audits*, as silly as that might sound it is a good idea as there is a lot to keep up with.

This is a required audit to help assure you are doing the dozen or so required audits, reviews and evaluations that you must do for HIPAA on an annual or more frequent basis. (In reality this is very close to an audit of you doing the MMM program, as all of these HIPAA requirements and more are met through the MMM each and every year, by the end of every year, PLUS all/any annual changes and updates obtained from attending the Washington DC Cybersecurity and HIPAA conference with all of the heads of the enforcement agencies).

When you originally completed the installation of your HIPAA program (one of ours or form another source) you should have done all of the originally needed audits, reviews and evaluations at that time, for that year.

The A-Z Audit checks to see these are done on an ONGOING basis.

If you have installed a complete initial HIPAA program and started the MMM program soon after, ALL WITHIN ONE YEAR OR LESS, then in answering A-Z Audit tool questions you will reference either the MMM modules you have done so far *OR* the particular audit/review/evaluation you did as part of your original initial HIPAA program installation.

If you have been on the MMM program one year or more then you will reference your latest MMM updates to answer the questions on the A-Z Audit tool.

The more complex issue is if you installed a new, complete HIPAA program a few years ago and then did not start the MMM until recently.

This means that if YOU HAVE NOT BEEN ON THE MMM PROGRAM FOR AT LEAST 12 MONTHS TO BE TOTALLY CAUGHT UP, FOR SOME MONTHS, YOU MAY ONLY HAVE THOSE ORIGINAL, OLD, INSTALLATION AUDITS/REVIEWS/EVALUATIONS TO REFERENCE, THAT ARE OUTDATED.

Therefore, if a section referenced in this A-Z Annual Audit has not been done since the installation of your original program, it may be acceptable to simply notate that it was done some time back and is scheduled to be updated within the next few months, and wait for the MMM to catch you up!

Ex. If you installed a program in January of 2017 and started doing MMM modules in April of 2020 and it is now September 2020, that would mean you have completed 6 MMM modules that would have acted to update 6 of the key audits/evaluations or reviews from your original installation, but it would leave several key audits/reviews and evaluations, referenced in the A-Z Audit, that have NOT yet been updated. This is where you might state it is NOT done, but scheduled in the next few months. Then next year, when this A-Z Audit comes around again, it will all be current. Depending on the 'tardy' audit topic, you may decide you need to catch one or two up immediately. If that is the case you can consult your original program to see what needs to be done.

In preparation for performing the audit:

Designate who is in charge of the annual audit. (At times **periodic** audits are performed by IT people and typically relate to new or altered software and hardware policies, procedures, protections, etc.) However, Senior management must be involved in this A-Z Annual Audit.

The easiest way to perform an annual audit/evaluation is to ask a series of questions to your audit team (consisting of one or more individuals and always including upper management). Answer the questions objectively and honestly and then propose updates to be added/performed/implemented - **including the anticipated completion date, whether days, weeks or months.**

Record those items be accomplished as **corrective actions** and include them in your HIPAA compliance manual so that proper follow up is performed.

This is a sample A-Z Audit. Components may or may not apply to your specific practice.

Annual A-Z Audit TOOL (Evaluation Form)

Date_____ Clinic Name_____
Next Audit Date_____

Who participated in this annual audit
(ex. Was senior management involved in the audit process?)
__YES __NO _____(name)

Was there an individual designated to oversee the audit?
__YES __NO _____(name)

Annual Security In-service (training) policy and procedure has been reviewed.
__YES__NO
Changes needed_____

Annual security in-service has been performed and participants documented.
__YES__NO

Additional topics , listed below, have been added for future in-service training.
_____
_____
_____

Risk analysis policies and procedures has been reviewed and the following topics/areas need improvement or further review.
_____
_____
_____

The list of clinic/practice assets has been reviewed and additions added as needed.
__YES__NO

The list of practice assets and potential threats has been updated with new solutions purposed.
__YES__NO

The next full risk analysis review relative to performance of GAP analysis and implementation of solutions, etc. is _____

The policy and procedure for the contingency plan Disaster RECOVERY procedures has been reviewed.
__YES__NO

The Disaster Recovery procedures, as outlined in the risk analysis (or a separate document), have been tested (by round table discussion) successfully with the proper staff involved and any appropriate updates have been instituted and documented.
__YES__NO

The Emergency Mode OPERATIONS procedure has been reviewed and modified as needed.
__YES__NO

The Emergency Mode plan has been trained to and tested with, all key personnel involved and documented.
__YES__NO

The equipment/software/procedures that are in place, to accomplish adequate records disposal, have been reviewed and are adequate.
__YES__NO

The policies to protect physical safety and security of all mobile devices has been reviewed and an inventory list is in place and functioning to track the whereabouts of the equipment and protect PHI.
__YES__NO

Policies and procedures are in place to restrict access to all secured areas. Computer screens are protected by repositioning/using rapid timeouts/computer screens or other means and have been protected from environmental hazards and theft, etc.
__YES__NO

Intrusion detection processes, encryption, access and authentication controls, etc. have been installed and are working.
__YES__NO

A copy of the 'system restore procedure' (data recovery) has been given to at least one person off site for use in case of emergency.
__YES__NO

Multiple backups are in place and functional.
List _____
__YES__NO

Encryption is in place and functioning for data at rest and for data being transmitted from or to any office device containing PHI.
__YES__NO

The maintenance log/checklist is up to date and all follow up is current.
__YES__NO

Strong passwords are in place and never shared among workforce = one password per person.
__YES__NO

Multiple layers of PHI access protection are in place, above and beyond just passwords. List_____
__YES__NO

Email is encrypted or not used for transfer of PHI, unless the patient has been told that email is not secure and they have given their permission anyway.
__YES__NO

Annual and periodic training is held for updating workforce relative to protection of PHI.
__YES__NO

Appropriate audit logs, needed for protecting our practice PHI, have been activated and are tracked, reviewed and actionable. Policies and procedures for all items are written and in place.
__YES__NO

ISAR's were performed periodically throughout the year.
__YES__NO

The workforce has been educated relative to the sanctions policy relating to protection of PHI.
__YES__NO

All devices that send or receive PHI have proper encryption.
__YES__NO

I have written a formalized checklist for a periodic information systems activity review and placed it in the HIPAA compliance manual.
__YES__NO

Information systems activity reviews have been performed and the results with corrective actions placed in the HIPAA compliance manual.
__YES__NO

Periodic reminders regarding issues that are of most importance in our office are being distributed on a monthly basis.
__YES__NO

There is a P & P regarding performing of this annual evaluation in the HIPAA compliance manual.
__YES__NO

This audit tool, for the annual audit/evaluation, has been modified to cover all requirements relative to this office and P & P's have been written for each item.
__YES__NO

Security Incident Procedures (procedure for reporting, investigating, addressing and reviewing security incidents) are written, any incident have been resolved and workforce has been educated.
__YES__NO

The two minimum necessary rules are being followed. (regarding access of data being limited by job description and only the minimum information being released regarding requests)
__YES__NO

Notice of patient privacy practices are being GIVEN to every new patient, we are obtaining signed attestations that they have received them and notices are available (displayed) in the office.
__YES__NO

A physical plant audit was conducted this year.
__YES__NO

Our mitigation plan/policy for accidental/incidental exposure has been reviewed with staff.
__YES__NO

A comprehensive review of all HIPAA policies was accomplished as differing parts of other audits or in total during this year.
__YES__NO

Staff has been trained to spot phishing attempts to circumvent our electronic security.
__YES__NO

Staff has been made aware to not post on or respond to any social media where a patient is involved (including responding to 'bad GOOGLE reviews' etc.)
__YES__NO

All needed BAA agreements are in place.
__YES__NO

All patient data was certified as cleaned from hard drives of any electronic device prior to disposing of the equipment.
__YES__NO