HIPAA Audit Checklist

618 TDO KB October 9, 2025 HIPAA 12.42K

HIPAA Audits: A Nine-Step Checklist

Here are nine tips to help you prepare now in case your dental practice is chosen for a HIPAA audit.

True, not every dental practice will get audited, but if your practice is covered by HIPAA you should take these steps anyway. They can help you make sure your HIPAA compliance program is in good shape. Remember, if someone submits a complaint to the government about your HIPAA practices, or if you have a reportable breach, OCR may respond with a compliance review or investigation.

Are these nine tips everything you need to do to get your HIPAA compliance up to speed? Well, no. But it's a pretty good start.

1. Watch For an Email From OCR

The Office for Civil Rights ("OCR") is using these email addresses to contact entities that might be audited:

os-ocr@hhs.gov

osocraudit@hhs.gov

Watch for these addresses, and if you get one of these emails, send a timely and accurate response. Check your spam filter to make sure a message from OCR hasn't been overlooked.

2. Practice Filling Out OCR's Pre-Audit Screening Questionnaire

OCR may send you a "Pre-Audit Screening Questionnaire." Why not fill it out now to make sure you have all the answers? The Questionnaire has sections for providers, plans, and business associates, and you only need to address the questions that would apply to you.

3. Review Your HIPAA Compliance Documents

Find your HIPAA compliance documents and make sure they're complete, up-to-date, and readily accessible.

Dental practices that get audited may have as little as **ten days** to submit their HIPAA compliance documents. OCR might ask for your:

- Security risk analysis (also called a "risk assessment") – see Tip 6 for more on this
- Security, Privacy, and Breach Notification policies and procedures
- Notice of privacy practices and acknowledgements of receipt
- Training records

- Sanctions imposed on workforce members for noncompliance
- Breach notification letters
- Business associate agreements
- Other HIPAA documents (authorization forms, documentation of complaints, etc., etc., etc.)

Remember: the retention period for HIPAA documents is at least six years from the date the document was created, or at least six years from the date the document was no longer in effect, whichever is later. Make sure you retain prior versions of yourHIPAA compliance documents for the appropriate period of time.

Once you submit your documents to OCR, you may not be able to submit additional information, explanations, or documentation. And obviously, you won't be able to update them after you receive the request from OCR. Make sure your documents are complete, up-to-date, and accessible now.

4. List Your Business Associates

Audited dental practices may be asked for a list of their business associates. Why not compile the list now, and make sure you have an up-to-date business associate agreement in place with each of them?

5. Review the HIPAA Audit Protocol

OCR released the protocol that HIPAA auditors will use when they audit covered providers, health plans, clearinghouses, and business associates.

Ok, it's really long, but don't freak out. Not all of it will apply to you, and you probably won't need to read all of the information in every single column (yes, it's in columns – didn't you click on the link?).

Column 1 just tells you which HIPAA rule you're in (Privacy, Security, or Breach Notification).

Focus on Column 5, which is labeled "Audit Inquiry." That's where you'll find the questions the auditors will ask. For example, the first question is:

> Does the health plan use or disclose for underwriting purposes, "Genetic Information" as defined at § 160.103, including family history?

If you're not a health plan, you can skip that one and move on to the second Audit Inquiry question:

> Do the covered entity's policies and procedures protect the deceased individual's PHI consistent with the established performance criterion?

Now, look at your HIPAA Privacy policies and procedures (Column 1 tells you this is a HIPAA Privacy question). Do your policies and procedures protect the PHI of deceased individuals in compliance with HIPAA? Here's an example of what that might look like:

Our dental practice protects deceased patients' PHI. Here are our procedures for responding to requests for information about deceased patients:

- Disclosure to a personal representative. HIPAA requires disclosure to the personal representative of a deceased patient. Verify the personal representative's identity and authority if you don't know him or her personally, and ask the personal representative to fill out our dental office's "Request for Access" form if he or she wishes to view or get copies of the deceased patient's PHI.

- Executor or Administrator. You may release the deceased patient's PHI to a legally authorized executor or administrator, or a person who is otherwise legally authorized to act on the behalf of the deceased patient or the estate. Ask the individual to provide documentation of his or her status as executor or administrator. If you don't know the individual personally, verify his or her identity. If the executor or administrator wishes to view or get copies of the deceased patient's PHI, ask him or her to fill out our dental office's "Request for Access" form.

- Permitted uses and disclosures. If a use or disclosure is permitted by HIPAA, authorization is not required.

- Uses and disclosures not permitted by HIPAA. If a use or disclosure is not permitted by HIPAA, the written authorization of the deceased patient's personal representative is required (this could be the deceased patient's executor or administrator – see above).

- Treatment. You may release the information for treatment purposes without a written authorization (for example, to a health care provider who is treating a member of the deceased patient's family).

- Individuals who were involved in the deceased patient's care or payment for care. You may, but you are not required to, disclose information about a deceased patient to a family member, relative, close personal friend, personal representative, or an individual who was responsible for the deceased patient's care, as long as (1) the person was involved in the deceased patient's care or payment for care, (2) the information is relevant to that person's involvement in the deceased patient's care or payment for care, and (3) the deceased patient did not express any preference against the disclosure.

- HIPAA no longer applies to patient information 50 years after the patient's death.

If your state has laws that are more stringent than HIPAA, make sure your policies and procedures comply with those laws, too. Next, move on to the next question in the "Audit Inquiry" column (lather, rinse, repeat).

If a question in the "Audit Inquiry" column doesn't ring a bell, Columns 2, 3 and 4 tell you where to look in the HIPAA Rules for that particular requirement.

6. Make Sure Your HIPAA Security Risk Analysis Really is a HIPAA Security Risk Analysis

If you've gone through the HIPAA Security Rule's administrative, physical and technical safeguards and written down how your dental practice complies with each one, *you may not have done a proper HIPAA Security risk analysis*!

The risk analysis (it's in §164.308(a)(1)(ii)(A)), which must be accurate and thorough, needs to focus on each electronic information assets that you use to create, maintain or transmit electronic PHI, and for each of these information assets you need to analyze vulnerabilities and threats and assess the risk in terms of likelihood and severity (hang in there – we'll provide a sample).

HIPAA requires you to use your risk analysis to implement security measures that are sufficient to reduce the risks and vulnerabilities to a reasonably appropriate level. This is sometimes referred to as a "risk management plan" (it's in §164.308(a)(1)(ii)(B)).

Here's a sample of ***a small part*** of a HIPAA security risk analysis – remember, your risk analysis needs to be accurate and thorough, meaning it covers foreseeable vulnerabilities and threats to *all*of your electronic information assets that create, store and transmit electronic PHI. We've added an extra column on the right for information about the risk management plan.

---

[1]Even though it may not fulfill the requirements of a proper risk analysis, looking at each HIPAA Security safeguard and documenting how your practice complies might help fulfill these other HIPAA Security obligations:

- Perform a periodic technical and nontechnical evaluation of the extent to which your policies and procedures meet HIPAAsecurity requirements (this is sometimes called a "gap analysis" – the requirement is in §164.308(a)(8) of the Security Rule).
- Assess each "addressable" safeguard to determine whether it's reasonable and appropriate for electronic information assets in your dental practice (and explain why or why not) – if it is, you have to implement it. If it's not, you have to explain what you will do instead. Document all of the above. The rules for addressable safeguards are in §164.306(e)(1) of the Security Rule.

Sample Partial HIPAA Security Assessment

What is “ransomware”? Bad guys use ransomware to encrypt your data, then they demand ransom to restore the data. Ransomware can be delivered through a “phishing” email or by exploiting a technical weakness in your system.

Don’t know enough about ransomware? Check out the resources from the ADA and the FBI:

- ADA Protect Your Business from Ransomware
- FBI Ransomware
- FBI Incidents of Ransomware on the Rise: Protect Yourself and Your Organization

Don’t know enough about phishing? Check out this resource from the Federal Trade Commission

- FTC Phishing

7. Read about the Audit Program on the OCR Website

The OCR website has a sample email (the kind you *don't* want getting caught in your spam filter) and helpful Q&A's about how they'll pick who gets audited, what happens during and after an audit, and who pays the auditors (spoiler alert: they do).

8. Do a Mock Audit

Many audits will be "desk audits," which means that the auditor will review documents you submit but won't visit your dental practice. However, some audits will be on-site audits, which will be conducted over three to five days, depending on the size of your practice. Obviously, on-site audits will be more comprehensive than desk audits and will cover a wider range of HIPAArequirements.

Tips 3, 4, 5 and 6 can help you prepare for a desk audit as well as for an on-site audit. If you'd like to take additional steps to help prepare for an on-site audit, why not do some role-playing exercises? For example, your staff might take turns asking each other questions from the HIPAA audit protocol, find the answers in your dental practice's HIPAA compliance documents, and demonstrate how your dental practice complies with HIPAA.

9. Work Hard, But Don't Panic

Your HIPAA compliance program should be very good, but it may not need to be absolutely perfect. OCR has said that the HIPAAaudits are mainly a compliance improvement activity to help OCR understand compliance efforts and determine what kinds of help they should provide and what kinds of corrective action would be most helpful.

However, if the auditors discover a serious compliance issue, OCR has stated that it may initiate a compliance review to further investigate.

Even though OCR doesn't plan to post a listing of the entities that get audited or the findings of an individual audit that clearly identifies the audited entity, OCR may need to release audit notification letters if there's a FOIA request ("FOIA" stands for the Freedom of Information Act).

And as you know, HIPAA breaches involving 500 or more individuals get posted on the so-called "Wall of Shame," which you can mine for "lessons learned" – and for motivation.

Protect your patients and your practice. Get started today.

Disclaimer

This resource is designed to assist dental practices in developing their HIPAA compliance program. In making these materials available, the ADA does not, nor does it intend to, provide legal or professional advice. Nothing here represents ADA's legal or professional advice as to any particular situation you may be facing. To get appropriate legal or professional advice, you need to consult directly with a properly qualified professional or with an attorney licensed to practice in your jurisdiction.

This resource discusses only federal, and not state law. Each dental practice must be aware of and comply with applicable state laws. This resource refers to federal statutes and regulations adopted by

agencies such as the U.S. Department of Health and Human Services (HHS). However, these materials have not been approved by HHS or any other federal agency. Dental practices vary widely, and each should develop and implement a compliance program appropriate to its circumstances and in compliance with all applicable laws and regulations.

The law varies from jurisdiction to jurisdiction, and it sometimes changes more rapidly than these materials. For that reason, we make no representations or warranties of any kind about the completeness, accuracy, or any other quality of these materials or any updates, and expressly disclaim all warranties, including all implied warranties (including any warranty as the merchantability and fitness for a particular use).

To the extent we have included links to any website, we intend no endorsement of their content and imply no affiliation with the organizations that provide their content. Nor do we make any representations or warranties about the information provided on those sites, which we do not control in any way.

© 2016 American Dental Association. All Rights Reserved.

6/9/2016

Online URL: https://kb.tdo4endo.com/article.php?id=618