ZenGRC

Preparing for a HIPAA audit

A Step-by-Step Guide

www.ZenGRC.com

Getting notified of an impending Health Information Portability and Accountability Act (HIPAA) audit can be a nerve-wracking experience.

You may not know precisely why you are being audited, and you probably will not have much time to prepare. The penalty for failure can be steep—findings of noncompliance by the U.S. Department of Health and Human Services Office for Civil Rights (OCR)—can incur fines of as much as $25,000 per single record compromised.

Most who pay these fines do so because they are not ready when the auditors knock on their door. Too often, health care providers and other processors of personal health information (PHI) delay preparing for an audit until the OCR's letter of notification arrives—too little, too late.

Rarely has the word "proactive" held so much weight. If your enterprise collects, processes, or stores PHI, it will be audited at some point. When that time comes, will you be prepared?

This checklist can help you say "yes," confidently.

Who gets audited

HIPAA AUDIT SUBJECTS FALL INTO TWO OVERARCHING CATEGORIES:

COVERED ENTITIES
such as medical and dental offices and hospitals that create, modify, and alter personal health records (PHRs)

BUSINESS ASSOCIATES,
which are third parties such as software companies or medical records companies that manage and store PHRs

Although both types of health information processors are subject to audits, OCR holds the covered entities ultimately responsible for the compliance of any business associates. Therefore, it is essential that covered entities ensure that their business associates handle PHI in accordance with HIPAA rules.

In other words, if you qualify as a “covered entity,” it behooves you to know as much about your business associates’ PHI privacy and security practices as you know about your own.

Why audits happen

If your enterprise gets audited, it will be for one of three reasons:

1. OCR selected you for one of its periodic random audits.

2. You have experienced a breach and reported it to OCR.

3. Someone has filed a complaint about your PHI practices.

What auditors are looking for

HIPAA's rules fall into two categories—privacy and security—in three areas:

- **ADMINISTRATIVE SAFEGUARDS**
- **PHYSICAL SECURITY**
- **TECHNICAL (CYBER) SECURITY**

The OCR may ask questions in each category:

Privacy:

- Have all your patients signed your privacy policy?
- Do your patients understand why you are collecting their information and what you plan to do with it?
- Have they agreed that you may process, store, and use their information?
- If patients ask who has viewed their records and when, can you show them?
- Can you honor patients' requests to hide their records from view or remove them from your database?
- Have you trained your workforce in the proper handling of PHI?
- Do you have appropriate process documents and evidence to support your answers to these questions?

Security:

- Do you have strong security controls around the PHI you store? This might include mobile and email encryption, firewalls, multi-factor authentication, and workforce security training and testing.
- Do you limit access to patient information on an as-needed basis?
- Have you experienced any breaches of PHI? If so, did you remedy the causes?

Preparing for an audit:

Step by step

1. Stay on task.

To ensure that your office or organization is prepared for—and will pass—an OCR audit, work on your policies and procedures, and monitor your compliance throughout the year, not just at audit time.

2. Audit yourself.

Self-audits are key to HIPAA success. Conduct them periodically—semi-annually or even quarterly—by engaging your own internal auditor, procuring the help of a third party, or using a quality governance, risk, and compliance (GRC) software.

3. Gather your documents.

Showing documentation of an internal audit, along with evidence that you have mitigated any issues, will go a long way toward helping you avoid or reduce fines if the OCR conducts an audit, even if you have experienced a data breach.

OTHER DOCUMENTS TO HAVE AT HAND FOR AUDITORS INCLUDE:

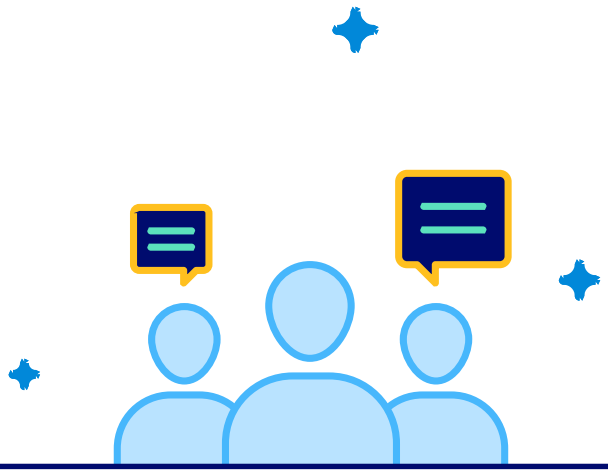
- Your **risk assessments/analyses**, **risk register**, and **risk management** plans. Make sure these are complete. In the OCR's first phase of HIPAA audits, 66 percent of entities did not have thorough and up-to-date risk assessments in place.
- HIPAA and security **training manuals** and **records of training**
- **Breach policy and response system** to show that everyone understands their roles and duties before, during, and after a cybersecurity incident
- **Proof of technical controls**, including data encryption, systems and network
- monitoring, and firewalls
- **Proof of adequate physical security** of your perimeter and premises
- **Business continuity plans**

4. Talk to your people.

Federal auditors will do more than scrutinize your documents. They will also talk to workers to ensure that your privacy, security, and risk policies and procedures are not only in place, but also being followed. You should do the same.

ASK YOUR EMPLOYEES:

- Are all patients signing a HIPAA privacy policy that clearly spells out what you can and can't do with their data?
- Are you doing what you say you will do, and no more, with patient data?
- Are you keeping records so that if a breach occurs, you can notify all affected data owners?
- Are you keeping records to enable you to answer any and all questions a patient might have about how you handle their data?
- Are you doing what you say you will do, and no more, with the entrusted patient data?
- Are you keeping records so that if a breach occurs, you can notify all affected data owners within the timeframes required by your BAA?
- Are you keeping records to enable you to answer any and all questions a patient might have about how you handle their data should the records be requested by the covered entity?
- Do you have a full record of any and all changes to protected health information (PHI)?



5. Mitigate issues.

THE MOST COMMON PROBLEMS THE OCR FINDS IN HIPAA AUDITS INCLUDE:

- The organization lacks a risk assessment/analysis and/or risk management plan. This finding incurs the highest OCR fines.
- Information security measures are insufficient. For example, data may not be encrypted, or may use an insufficient encryption method.
- The organization has not documented its policies and processes, or fails to follow its documented policies and procedures.

To avoid fines, your organization must show evidence of both due diligence and "due care"—that you did the appropriate research and implemented the correct policies and processes, and that you are monitoring and following these processes.

Perhaps the most preventable error, however, is negligence.

BREACHES HAPPEN. THE AUDITORS KNOW THIS AND LIKELY WILL NOT PENALIZE YOU IF, AFTER A BREACH, YOU:

- Notify the OCR of the breach
- Notify the affected data owners
- Work to minimize the breach's impact on all affected parties
- Resolve the incident according to your policies
- Assess the cause and adjust your risk register
- Take measures to prevent a recurrence
- Document your handling of the breach

If, on the other hand, you do not report a breach or simply ignore its occurrence—and this happens more often than you might think—you will be far more likely to incur penalties.

6. Keep calm.

SITTING FACE-TO-FACE WITH AUDITORS AND ANSWERING THEIR QUESTIONS CAN BE THE MOST DIFFICULT PART. HERE ARE SOME TIPS TO HELP YOU WEATHER THE INTERVIEW GRACEFULLY:

Answer only what you are asked.

As on the witness stand, try to refrain from volunteering information. Even if you have nothing to hide, rattling on can raise red flags and cause the auditor to dig more deeply.

Get comfortable with silence.

As a technique to extract more information, auditors may let you answer the question and then count (internally) to ten. Long periods of silence make most people uncomfortable, causing them to rush to fill the void with chatter. Resist the urge to continue talking.

Tell the truth.

Answer as truthfully as you can. If you don't know the answer to a question, say so. "I don't know, but I'll find out and get back to you" is a perfectly adequate response—as long as you follow through.

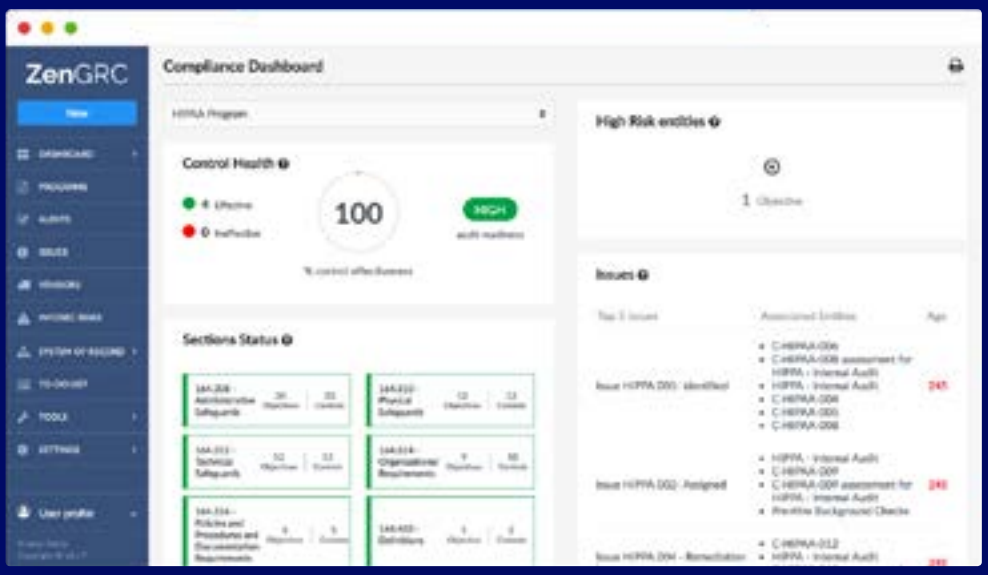
No matter how well prepared you are, an audit can still be an anxiety-producing experience.

An audit should be a fairly simple and straightforward event for enterprises that have taken HIPAA seriously from day one, formulated risk analyses and risk management plans, documented issues and taken steps to remedy them, trained employees in HIPAA requirements, and prioritized the privacy and security of patient data.

If your enterprise has fallen behind the curve, however, you still need not despair.

If you feel unprepared for a HIPAA audit, now is the time to get your affairs in order—before you get that letter or email announcing an impending audit.

Why not turn over a new leaf? Follow these recommendations, set up quarterly or semi-annual self-audits to ensure continued compliance, and then relax. There are so many things in business, as in life, that we can't control—but you've got this. And if you need help, don't worry: There's a tool for that.



The Checklist

Privacy

- ◯ Have all your patients signed your privacy policy?
- ◯ Do your patients understand why you are collecting their information and what you plan to do with it?
- ◯ Have they agreed that you may process, store, and use their information?
- ◯ If patients ask who has viewed their records and when, can you show them?
- ◯ Can you honor patients' requests to hide their records from view or remove them from your database?
- ◯ Have you trained your workforce in the proper handling of PHI?
- ◯ Do you have appropriate process documents and evidence to support your answers to these questions?

Security

- ◯ Do you have strong security controls around the PHI you store? This might include mobile and email encryption, firewalls, multi-factor authentication, and workforce security training and testing.
- ◯ Do you limit access to patient information on an as-needed basis?
- ◯ Have you experienced any breaches of PHI? If so, did you remedy the causes?

PREPARING FOR AN AUDIT: STEP BY STEP

1. Stay on task.

2. Audit yourself.

3. Gather your documents.

Documents to have at hand for auditors include:

- ◯ Results of your internal HIPAA audit.
- ◯ How you mitigated the issues your internal audit found, if any.
- ◯ Your risk assessments/analyses, risk register, and risk management plans. Make sure these are complete. In the OCR's first phase of HIPAA audits, 66 percent of entities did not have thorough and up-to-date risk assessments in place.
- ◯ Employee HIPAA and security training manuals and records of training
- ◯ Breach policy and response system to show that everyone understands their roles and duties before, during, and after a cybersecurity incident
- ◯ Proof of technical controls, including data encryption, systems and network monitoring, and firewalls
- ◯ Proof of adequate physical security of your perimeter and premises
- ◯ Business continuity plans

4. Talk to your people.

Ask your employees:

- ◯ Are all patients signing a HIPAA privacy policy that clearly spells out what you can and can't do with their data?
- ◯ Are you doing what you say you will do, and no more, with patient data?
- ◯ Are you keeping records so that if a breach occurs, you can notify all affected data owners?
- ◯ Are you keeping records to enable you to answer any and all questions a patient might have about how you handle their data?
- ◯ Are you doing what you say you will do, and no more, with the entrusted patient data?
- ◯ Are you keeping records so that if a breach occurs, you can notify all affected data owners within the timeframes required by your BAA?
- ◯ Are you keeping records to enable you to answer any and all questions a patient might have about how you handle their data should the records be requested by the covered entity?
- ◯ Do you have a full record of any and all changes to protected health information (PHI)?

5. Mitigate issues.

The most common problems the OCR finds in HIPAA audits include:

- ◯ The organization lacks a risk assessment/analysis and/or risk management plan. This finding incurs the highest OCR fines.
- ◯ Information security measures are insufficient. For example, data may not be encrypted, or may use an insufficient encryption method.
- ◯ The organization has not documented its policies and processes, or fails to follow its documented policies and procedures.

6. Keep calm.

About ZenGRC

Founded in 2009, ZenGRC has reimagined bulky legacy GRC software to meet the demands of today's dynamic data-driven ecosystem. The company is recognized for its forward-thinking cloud platform, ZenGRC, that elevates risk, compliance, and audit from a burdensome expense to a strategic advantage. ZenGRC is headquartered in San Francisco.

Contact a ZenGRC expert today to request your **free demo**, and embark on the worry-free path to regulatory compliance—the Zen way.

www.ZenGRC.com/resources
engage@zengrc.com
(877) 440-7971