



## How to Prepare for and Respond to a HIPAA Audit

- The Office for Civil Rights (OCR) oversees HIPAA and enforces it through investigations and audits.
- Covered entities and business associates should prepare for a potential audit or investigation to ensure they can pass.
- During the last audit phase in 2017, OCR found widespread noncompliance. The key problems identified were a lack of **risk analysis**, noncompliance with the **patient right of access rule**, and deficient **breach notification content**.
- OCR plans to begin audits again to assist regulated entities in improving their HIPAA compliance and their protection of health information.

How to **prepare** for an audit or investigation:

- Review, update, and document your HIPAA Risk Analysis.
- Review and update your policies to reduce risks and fully comply with the HIPAA Privacy, Security, and Breach Notification Rules.
- Refresh workforce training; include general HIPAA training and cybersecurity awareness; document the training.
- Update procedures and responsibilities to comply with the patient right of access rule.
- Review and update breach notification procedures.
- Review the latest guidance about preventing cybercrime and make improvements where needed. (e.g., [StopRansomware.gov](https://www.stopransomware.gov), and the [HHS Cybersecurity Performance Goals](#))

How to **respond** to an audit or investigation:

- Cooperate.
- Answer questions promptly.
- Provide documentation requested.
- Accept technical assistance or guidance if offered by OCR.

Organizations that cooperate and show a willingness to improve their compliance do much better in investigations and audits. The process will take less time and, in the case of an investigation, will be less likely to result in a civil money penalty or a high settlement amount.

*If you have a question or need help, let us know:*

[info@hipaaetool.com](mailto:info@hipaaetool.com) or **800-570-5879**