Attinkom
We verify your trust

Demystifying HIPAA Compliance

©Copyright 2022 Attinkom. All Rights Reserved.

Attinkom
We verify your trust

This publication contains general information only and Attinkom is not, by means of this publication, rendering any professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Attinkom shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, "Attinkom" means Attinkom LLC. Please see https://attinkom.com and email us at info@attinkom.com for any specific services that you may be looking for.

©Copyright 2022 Attinkom. All Rights Reserved.

Attinkom
We verify your trust

Table of Contents

1. What is HIPAA compliance?
2. What is the difference between PHI and ePHI?
3. Who needs to comply with HIPAA?
4. What Are the Rules?
5. HIPAA Enforcement
6. Role of Cybersecurity
7. How do you comply with HIPAA?
8. How is HIPAA audited?
9. Stay updated on HIPAA changes
10. Is a SOC 2 Report HIPAA Compliant?
11. Closing thoughts

©Copyright 2022 Attinkom. All Rights Reserved.

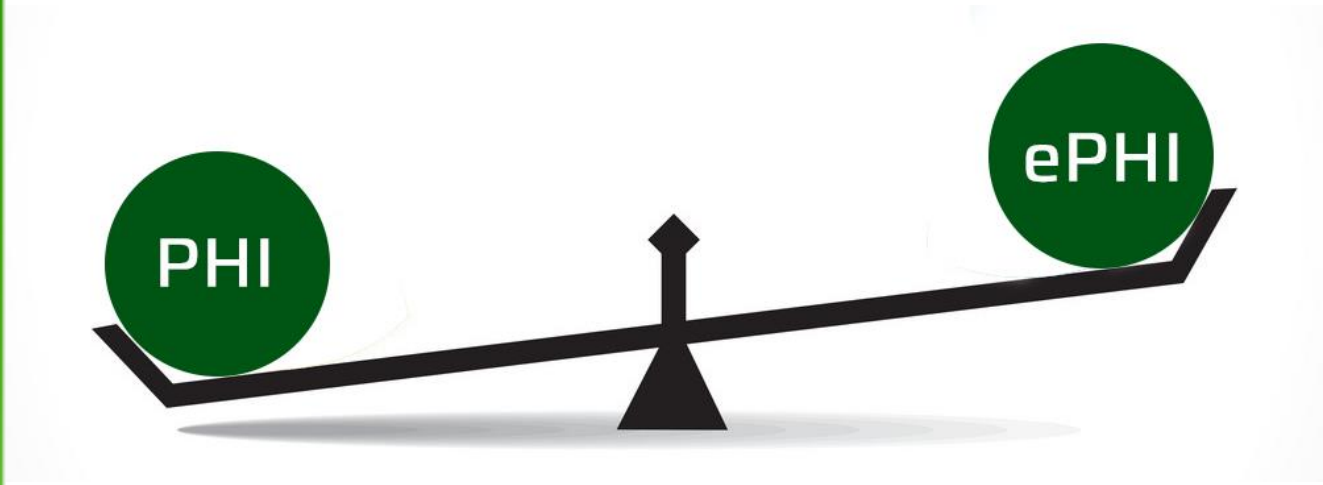
Attinkom
We verify your trust

What is HIPAA compliance?

The Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA, is a series of regulatory standards that outline the lawful use and disclosure of protected health information (PHI).

Under HIPAA PHI is considered to be any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a healthcare clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the provision of healthcare or payment for healthcare services. Protected health information (PHI) is any demographic information that can be used to identify a patient or client of a HIPAA-beholden entity. Common examples of PHI include names, addresses, phone numbers, Social Security numbers, medical records, financial information, and full facial photos to name a few.

©Copyright 2022 Attinkom. All Rights Reserved.



What is the difference between PHI and ePHI?

The difference between PHI and ePHI is that ePHI refers to Protected Health Information that is created, used, shared, or stored electronically – for example on an Electronic Health Record, in the content of an email, or in a cloud database. Both PHI and ePHI are subject to the same protections under the HIPAA Privacy Rule, while the HIPAA Security Rule and the HITECH Act mostly relate to ePHI.

Who needs to comply with HIPAA?

The two types of entities responsible for protected health information need to be HIPAA compliant — covered entities and business associates.

©Copyright 2022 Attinkom. All Rights Reserved.

Attinkom
We verify your trust

Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. If a covered entity engages a business associate to help it carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information. In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules.

If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA Rules.

©Copyright 2022 Attinkom. All Rights Reserved.

Attinkom
We verify your trust

A Covered Entity is one of the following:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.	This includes: • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service

©Copyright 2022 Attinkom. All Rights Reserved.

involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

©Copyright 2022 Attinkom. All Rights Reserved.

Attinkom
We verify your trust

What are the Rules?

HIPAA Privacy Rule

The HIPAA Privacy Rule sets national standards for patients' rights to PHI. Some of the standards outlined by the HIPAA Privacy Rule include patients' rights to access PHI, health care providers' rights to deny access to PHI, the contents of Use and Disclosure HIPAA release forms and Notices of Privacy Practices and more.

The organization must document the specifics of the regulation in HIPAA Policies and Procedures. They also must train staff on these Policies and Procedures annually, with documented attestation.

HIPAA Security Rule

The HIPAA Security Rule sets national standards for the secure maintenance, transmission, and handling of ePHI. The HIPAA Security Rule applies to both covered entities and business associates because of the potential sharing of ePHI. The Security Rule outlines standards for the integrity and safety of ePHI, including physical, administrative, and technical safeguards that must be in place in any healthcare organization.

The organization must document the specifics of the regulation in HIPAA Policies and Procedures. They also must train staff on these Policies and Procedures annually, with documented attestation.

HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. The HIPAA Breach Notification Rule is a set of standards that covered entities and business associates must follow in PHI or ePHI data breaches. The Rule lays out different requirements for breach reporting depending on the scope and size.

Regardless of size, organizations must report all breaches but the specific protocols for reporting change depending on the number of records breached. We outlined the specifics of the HIPAA Breach Notification Rule in the sections below.

HIPAA Omnibus Rule

The HIPAA Omnibus Rule is an addendum to HIPAA regulation. It was enacted to apply HIPAA to business associates and to covered entities. The HIPAA Omnibus Rule mandates that business associates must be HIPAA compliant and outlines the rules surrounding Business Associate Agreements (BAAs).

Business Associate Agreements must be executed between a covered entity and business associate–or between two business associates–before transferring or sharing ANY PHI or ePHI.

©Copyright 2022 Attinkom. All Rights Reserved.

HIPAA Enforcement

HHS' Office for Civil Rights is responsible for enforcing the Privacy and Security Rules. Enforcement of the Privacy Rule began April 14, 2003, for most HIPAA covered entities. Since 2003, OCR's enforcement activities have obtained significant results that have improved the privacy practices of covered entities.

The corrective actions obtained by OCR from covered entities have resulted in systemic change that has improved the privacy protection of health information for all individuals they serve.

HIPAA covered entities were required to comply with the Security Rule beginning on April 20, 2005. OCR became responsible for enforcing the Security Rule on July 27, 2009.

As a law enforcement agency, OCR does not generally release information to the public on current or potential investigations.

©Copyright 2022 Attinkom. All Rights Reserved.

The OCR's role in maintaining medical HIPAA compliance comes in the form of routine guidance on new issues affecting health care and in investigating common HIPAA violations.

©Copyright 2022 Attinkom. All Rights Reserved.

Attinkom
We verify your trust

The Seven Fundamental Elements of an Effective Compliance Program

The HHS Office of Inspector General (OIG) created the Seven Elements of an Effective Compliance Program. These elements give guidance for organizations to vet compliance solutions or create their own compliance programs.

1. Implementing written policies, procedures and standards of conduct
2. Designating a compliance officer and compliance committee
3. Conducting effective training and education
4. Developing effective lines of communication
5. Conducting internal monitoring and auditing
6. Enforcing standards through well-publicized disciplinary guidelines
7. Responding promptly to detected offenses and undertaking corrective action

©Copyright 2022 Attinkom. All Rights Reserved.

Attinkom
We verify your trust

Role of Cybersecurity

A growing number of patient records reside in the cloud or other digital formats as healthcare organizations embrace technology. To ensure patient data is secure and safe, cybersecurity is of utmost importance. his This can be accomplished through an effective cybersecurity strategy, but to avoid complications or breaches of confidential data,

Leaked patient data can have financial and reputational repercussions. Negligence will result in financial penalties for your organization. Patients may not trust you to safeguard their sensitive information.

Naturally, your organization should prevent data breaches from occurring in the first place. If sensitive patient information falls into the wrong hands, or you believe that your organization is at risk for a cyberattack, the U.S. Department of Health & Human Service outlines how you should respond to cyberattacks:

Respond – The entity must execute response and mitigation procedures, contingency plans

Report Crime – The entity should report crime to criminal and law enforcement agencies.

Report Threat – The entity should report all cyber threat indicators to the appropriate federal agencies and ISAO's.

Assess Breach – The entity must assess incident to determine if there is a breach of protected health information.

©Copyright 2022 Attinkom. All Rights Reserved.

Attinkom
We verify your trust

How do you comply with HIPAA?

HIPAA regulation outlines a set of national standards that all covered entities and business associates must address.

HIPAA requires covered entities and business associates to conduct periodic technical and nontechnical audits of their organization to assess Administrative, Technical, and Physical gaps in compliance with HIPAA Privacy and Security standards.

Under HIPAA, a Security Risk Assessment is not enough to be compliant –it's only one essential audit that HIPAA-beholden entities are required to perform to maintain their compliance year-over-year.

Covered entities and business associates must develop Policies and Procedures corresponding to HIPAA regulatory standards. These policies and procedures must be regularly updated to account for changes to the organization.

©Copyright 2022 Attinkom. All Rights Reserved.

Annual staff training on these Policies and Procedures is a best practice. There should be documented employee attestation stating they have read and understood the organization's policies and procedures.

HIPAA-covered entities and business associates must document ALL efforts they take to become HIPAA compliant. This documentation is critical during a HIPAA investigation with HHS OCR to pass strict HIPAA audits.
Covered entities and business associates must document all vendors with whom they share PHI. The entities and associates must ensure secure PHI handling to execute Business Associate Agreements. BAAs should be reviewed annually to account for changes to the nature of organizational relationships with vendors. BAAs must be executed before ANY PHI can be shared.

When a covered entity or business associate has a data breach, they must document the breach and notify patients that their data was compromised in accordance with the HIPAA Breach Notification Rule.

©Copyright 2022 Attinkom. All Rights Reserved.

How is HIPAA audited?

Federal HIPAA auditors levy HIPAA fines on a sliding scale. Fines range from $100 to $50,000 per incident depending on the level of perceived negligence. Expect higher fines if auditors detect that the organization under investigation has neglected to perform a “good faith effort” toward HIPAA compliance. With well over $40 million levied in fines since 2016, HIPAA compliance is more important now than ever before.

The HIPAA compliance culture is built on a series of interlocking regulatory rules. In order to ensure the privacy, security, and integrity of protected health information, healthcare organizations should implement it.

©Copyright 2022 Attinkom. All Rights Reserved.

Stay updated on HIPAA changes

HIPAA compliance can be a moving target, with changes taking place on a regular basis. After implementing all the right cybersecurity measures and processes for responding to breaches, you'll still need to stay on top of new HIPAA developments. There are a variety of HIPAA changes expected to take effect in 2022 that you should prepare for now.

Some highlights of the 2022 HIPAA update include potential changes to:

1. Patient acknowledgment of notice of privacy practices
2. The minimum necessary standard for PHI protection
3. Allowable disclosures related to care coordination and case management
4. Disclosures of PHI for health emergencies
5. Citizens' rights to access their protected health information (PHI)
6. Fees that organizations may charge individuals to access PHI

It's crucial to monitor the upcoming HIPAA update in 2022 and work with your compliance partner to ensure compliance when it arrives, no matter if you've reached HIPAA compliance at present.

©Copyright 2022 Attinkom. All Rights Reserved.

Is a SOC 2 Report HIPAA Compliant?

Often, clients ask us if a SOC 2 report's scope meets HIPAA requirements. As a general rule, no, they are not, but it all depends on the scope of the audit.

A SOC 2 report, or Service and Organization Controls report, is used by service organizations to demonstrate to their clients and stakeholders the IT general and organizational controls that they have in place which secure the services they provide. The AICPA issues the guidance used to perform SOC 2 audits specifically AT-C 105 and AT-C 205. There are five Trust Services Criteria (TSCs) that can be included in a SOC 2 report based on the services provided by the service organization. The five criteria are:

- Security
- Availability
- Confidentiality
- Processing Integrity
- Privacy

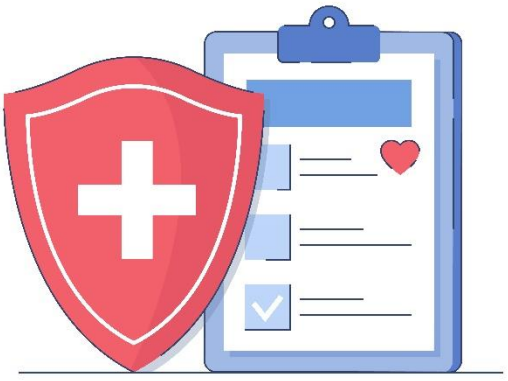
The only criteria that must be included in the SOC 2 report are the Security, or Common Criteria. All other criteria are added at the discretion of the service organization, with help from their auditor, when determining the scope of audit based on the services provided to their customers.

When looking at HIPAA compliance, a SOC 2 report focused on security is usually a good baseline for the controls that need to be in place. Additionally, additional controls should be considered. As a result of significant overlap between the SOC 2 and HIPAA Compliance reports, Attinkom typically performs both fieldwork for both. We issue two separate reports, one covering the SOC 2 criteria and the other covering HIPAA compliance.

©Copyright 2022 Attinkom. All Rights Reserved.

Closing thoughts

Also, we discussed the main objectives for undergoing a SOC 2 audit and a HIPAA Security Rule Compliance audit. There is overlap between the two reports, but their objectives and users are different. A SOC 2 provides a baseline for data security practices, but a HIPAA report has additional requirements that need to be met.



To find out more about how Attinkom can assist your organization in starting the process towards obtaining your SOC 2 or HIPAA Compliance reports, please contact us.

©Copyright 2022 Attinkom. All Rights Reserved.