Couchdrop

A COUCHDROP WHITE PAPER

HIPAA Compliance for Cloud Service Providers

Contents

Overview

With companies around the world seeing the benefits of cloud computing, most businesses now use some kind of cloud service as part of their business operations. Working in the cloud offers more flexibility, improved access to files, redundancy, security, and much more.

Privacy and security are a concern for all entities using or planning to use cloud services. But when it comes to working with data falling under HIPAA regulations, security, and privacy are paramount for ensuring that personal information is kept safe. To meet HIPAA requirements, there are several items and procedures that must be followed to legally process the data.

This white paper examines what HIPAA is and why additional security is required for this kind of data, along with what cloud service providers need to do to work with HIPAA data. It also includes some of the unique considerations entities should consider when choosing a cloud service provider for HIPAA-related data.

What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. It was signed into law in 1996 in the United States of America with the goal of expanding healthcare insurance coverage for United States citizens as well as enacting guidelines and restrictions on how Personally Identifiable Information (PII) and Protected Health Information (PHI) must be handled and protected.

The privacy portion of HIPAA is particularly important for any entities that have or will have access to PII and PHI, including Cloud Service Providers (CSP). It is vital for CSPs to safeguard customer data, but there are additional steps to ensure specific identifiers addressed in HIPAA are properly protected and meet all requirements.

What is considered Personally Identifiable Information?

PII is any information that can be used to identify a specific individual. This includes information such as:

- Name
- Date of Birth
- SSN and Passport Numbers
- Financial records
- Work history
- Anything else that can be used to denote an individual

While all of this information is important for CSPs to safeguard, HIPAA in particular is concerned with PHI.

HIPAA and PHI

A subset of PII, protected health information is defined by HIPAA are the following 18 identifiers:

1. Names
2. All geographic subdivisions smaller than a state (street address, city, county, zip code)
3. Dates, including birthdate, admission date, discharge date, and date of death
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web URLs
15. IP addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photos
18. Any other unique identifying number, characteristic, or codes

HIPAA compliance does not refer to all PII, but rather these 18 PHI identifiers. Only health information that can be traced back to an individual is covered by HIPAA; for instance, data used for research purposes where the health information has identifying information stripped and cannot be traced back to the specific individual may be shared with researchers and is no longer considered PHI.

What is the HITECH Act?

The electronic transmission of health information was one reason that HIPAA was signed into law. However, this was before the days of cloud computing, and as a result, further amendments have been made to HIPAA along with companion acts for advancements in technology such as the HITECH Act to address working with modern technology.

HITECH stands for the Health Information Technology for Economic and Clinical Health Act. It was passed into law in 2009 as part of the American Recovery and Reinvestment Act. This economic stimulus package was designed to improve infrastructure and encourage technological advancements in healthcare.

Who is covered by HIPAA and HITECH?

HIPAA applies to two different entities. The first are Covered Entities. These include healthcare plans, health clearinghouses, and healthcare providers that transmit any health information in electronic form.

The second are Business Associates. Business Associates provide a service or function on behalf of a Covered Entity relating to Protected Health Information.

Enforcement of the HITECH Act

Violating the HITECH Act carries penalties under the HITECH Act Enforcement Interim Final Rule. Penalties range in four tiers depending on whether a person violated the law by accident or willfully neglected adhering to the HITECH standards.

Notifying clients of a data breach

Under the HIPAA breach Notification Rule, both HIPAA-covered entities and Business Associates must provide notification if there is a breach of PHI. This includes any CSPs who store, transfer, or process PHI in any way.

HHS.gov uses a specific definition of what constitutes a breach. It is "an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information" and takes into consideration these factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

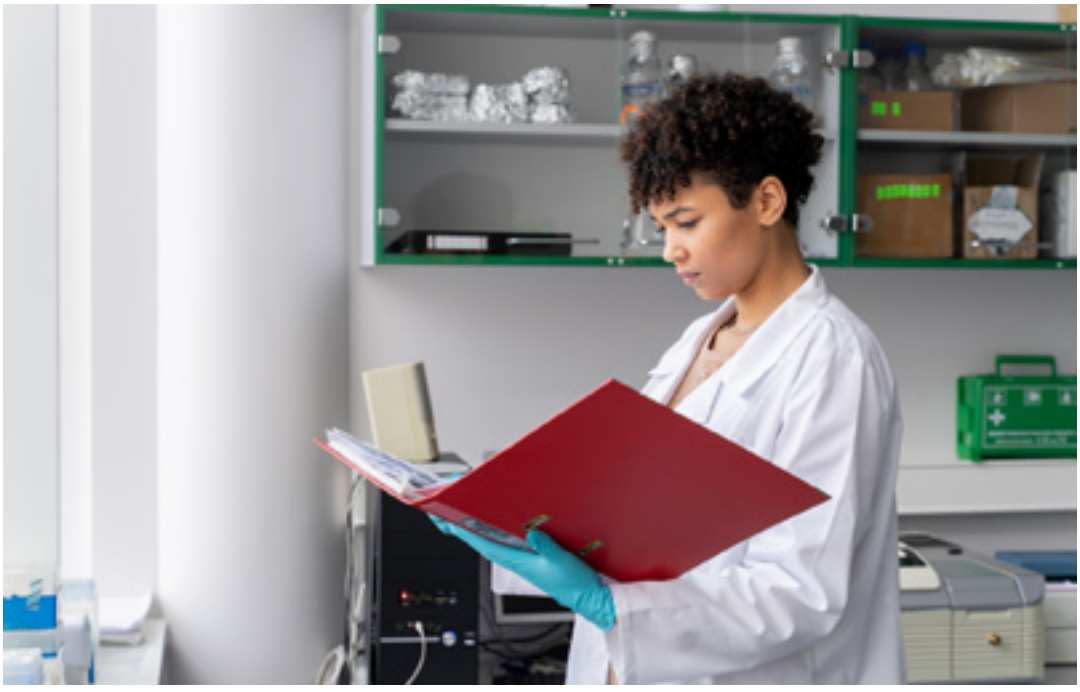
Along with notifying affected individuals, Covered Entities are required to notify the Secretary of breaches affecting over 500 individuals within 60 days by filling out and submitting a breach report form.

The HITECH and HIPAA Acts for CSPs

Part of the HITECH act included encouraging healthcare providers to transition to using electronic health records for better health outcomes. Electronic records are easier to store and retrieve, and files can be sent faster and easier between different providers when required.

Along with the recommendation, the HITECH Act strengthened the privacy requirements of HIPAA, including how any entity can send and store records containing PHI. These requirements pertain to CSPs like storage providers who store the records as well as the company that owns the data itself.

Consequently, a business that will store or access PHI through the cloud must ensure that the service provider is compliant with HIPAA and HITECH. This means that CSPs that store or transmit PHI needs to meet specific standards to be eligible to work with this kind of data.



HIPAA Compliance for CSPs

Currently there is no single standard for HIPAA compliance for CSPs. The final omnibus rule published in 2013 refined HIPAA so that Business Associates such as CSPs are also responsible for meeting HIPAA regulations, not only Covered Entities.

To ensure compliance with HIPAA regulations, CSPs have several responsibilities and standards to meet for risk analysis and management, data management, and breach notifications.

All CSPs must also include a Business Associate Agreement (BAA) if transferring or storing PHI data.

Risk Analysis and Management

To be eligible to store or transmit PHI, a CSP must meet standards for risk analysis and management.

A formal and comprehensive risk analysis is required where the CSP identifies potential risks specific to the PHI they plan to work with. The analysis should include what the risks are, the likelihood of a data breach, and a containment and notification plan should a data breach happen. The Security Risk Assessment Tool from HealthIT.gov is a downloadable tool that can help guide CSPs through this process if needed.

A risk management plan explains how the CSP safeguards against each of the risks identified as well as other security protocols and procedures set in place. User Access Control, for example, could ensure that only members of a specific team have access to see or perform actions on PHI data.

Both the risk analysis and management plan must be updated periodically to check for new risks and any time there are updates to how risks are handled since the last analysis.

Update security protocols as needed

If the risk analysis plan shows there are gaps in security and that additional updates are needed to meet HIPAA standards, these updates must be made before the CSP can process any PHI.

A third-party audit is required annually for companies handling HIPAA data, and most businesses must keep logs of these audits for 6 years.

Include a Business Associate Agreement

A Business Associate Agreement (BAA) is required for all CSPs working with PHI. Specifics of Business Associates and BAAs are covered in the next section.

Business Associate Agreements

All Business Associates working with HIPAA data must include a Business Associate Agreement before working with PHI. A BAA is a formal, written agreement that specifies the responsibilities of the Covered Entity and the Business Associate for safeguarding PHI.

The official definition of a Business Associate for HIPAA is "a person or entity, other than a member of the workforce of a Covered Entity, who performs functions or activities on behalf of, or provides certain services to, a Covered Entity that involve access by the Business Associate to protected health information".

Under this definition, any CSP that transfers, stores, or processes PHI is considered a Business Associate. When working with PHI, it's in everyone's best interest to sign a BAA when unsure if it's required as failure to do so can result in heavy fines for involved parties.

Liability of Business Associates

Both Business Associates and Covered Entities are required to take steps to ensure that PHI is protected. Each party has their own set of liabilities and responsibilities.

According to HHS.gov, Business Associates like CSPs are directly liable for the following HIPAA violations:

1. Failure to provide the Secretary with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the Secretary to information, including protected health information (PHI), pertinent to determining compliance.
2. Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in an investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA Rules.
3. Failure to comply with the requirements of the Security Rule.
4. Failure to provide breach notification to a Covered Entity or another Business associate.
5. Impermissible uses and disclosures of PHI.
6. Failure to disclose a copy of electronic PHI (ePHI) to either (a) the Covered Entity or (b) the individual or the individual's designee (whichever is specified in the Business Associate Agreement) to satisfy a Covered Entity's obligations under 45 CFR 164.524(c)(2)(ii) and 3(ii), respectively, with respect to an individual's request for an electronic copy of PHI.
7. Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

8. Failure, in certain circumstances, to provide an accounting of disclosures.
9. Failure to enter into Business Associate agreements with subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for such agreements.
10. Failure to take reasonable steps to address a material breach or violation of the subcontractor's Business Associate agreement.

What must be included in a BAA

The specifics of the BAA will depend on the nature of the work and the relationship between the Business Associate (the CSP) and the Covered Entity using the cloud service. However, for a BAA to comply with HIPAA standards, it must address the following:

- Describe the required and permitted use of PHI by the Business Associate.
- Ensure that the Business Associate will not disclose or use PHI beyond the required or permitted use.
- Outline that the Business Associate will use appropriate safeguards to stop PHI from inappropriate use, access, or disclosure.

The cloud service provider must create a BAA for each client where HIPAA data is involved and the Covered Entity must agree to and sign the agreement.

A sample BAA can be found on the Business Associate Contracts page from HHS.gov.

Couchdrop's HIPAA and HITECH Compliant architecture

Couchdrop is a CSP specializing in file transfers and data movement. Couchdrop's unique approach of not storing data and integrating with external Cloud Storage engines like AWS S3 ensures that customers have complete control over their data. Additionally, Couchdrop's hosted storage utilizes AES256 encryption–and data in transit is encrypted using HTTPS (TLS 1.2 minimum) or SSH depending on the chosen transfer protocol. There is also the option to use an RSA 2048-bit key for data encryption which meets HIPAA and HITECH standards.

HIPAA-Compliant Architecture

Couchdrop doesn't store customer data at any stage. Instead, users connect their own storage and then use Couchdrop to transfer files between their connected storage. This gives heightened security and control to users.

But Couchdrop's HIPAA-Compliant Architecture goes even further. It is designed exclusively for customers moving HIPAA data. So how does this architecture differ from Couchdrop's standard offering? There are a few differences for heightened security and data protection.

One is that HIPAA data uses dedicated compute nodes located in the United States which are used exclusively for HIPAA customers. Data is processed in San Francisco and never leaves the United States.

Couchdrop's HIPAA cluster is housed in Amazon Web Services (AWS) due to their HIPAA-compliant options.

AWS will designate accounts specifically as HIPAA accounts and meets FedRAMP and NIST 800-53 that map to the HIPAA Security Rule. AWS also has a standard BAA for HIPAA clients as required for CSPs.

Couchdrop and HIPAA customers

Couchdrop works with many enterprise customers who rely on the HIPAA-Compliant architecture for file transfers. As a cloud-native MFT platform, Couchdrop's unique infrastructure offers many additional advantages and levels of protection.

Some of these advantages include:

- The ability to bring existing cloud storage like Dropbox, Google, SharePoint or Azure and transfer files between them as well as to and from local servers using SFTP.
- Data is not stored at any stage with Couchdrop.
- When a Couchdrop account is deleted, client site information and data are purged after 90 days.
- SOC2 compliance
- Granular access controls and optional features like static IPs and restricting transfer protocols to specific users allow for maximum control of data.
- Comprehensive access logs include logins, changes, transfer logs, and more.
- Inboxes and automations simplify file transfers and automate workflows to reduce manual file handling and minimize errors.

With fast, secure file transfers that are easy to set up and manage, Couchdrop is an excellent choice for companies needing to move HIPAA-related data.

Conclusion

The HIPAA and HITECH acts are comprehensive pieces of legislation designed to provide better health outcomes for people in the United States and protect their personal information. Electronic health records and improved file transfer protocols allow for information to be shared quickly and securely with relevant parties.

However, it is imperative that both Covered Entities and Business Associates including the cloud service providers they choose to work with put in place appropriate safeguards for protected health information. CSPs planning to work with PHI are liable for protecting this data and may need additional protocols for PHI compared to other data they process, along with creating a Business Associate Agreement for each client.

For HIPAA-compliant file transfers, Couchdrop's cloud-native managed file transfer platform offers fast and secure file transfers to cloud storage providers, NAS devices, on-premise servers, and more. Couchdrop creates a customized Business Associate Agreement for every HIPAA customer explaining how the data will be processed, how it is protected, and the responsibilities of both parties in safeguarding PHI on the Couchdrop platform.

To find out more about how Couchdrop works with HIPAA data or to enquire about using the HIPAA-compliant architecture, contact Couchdrop support or email support@couchdrop.io.