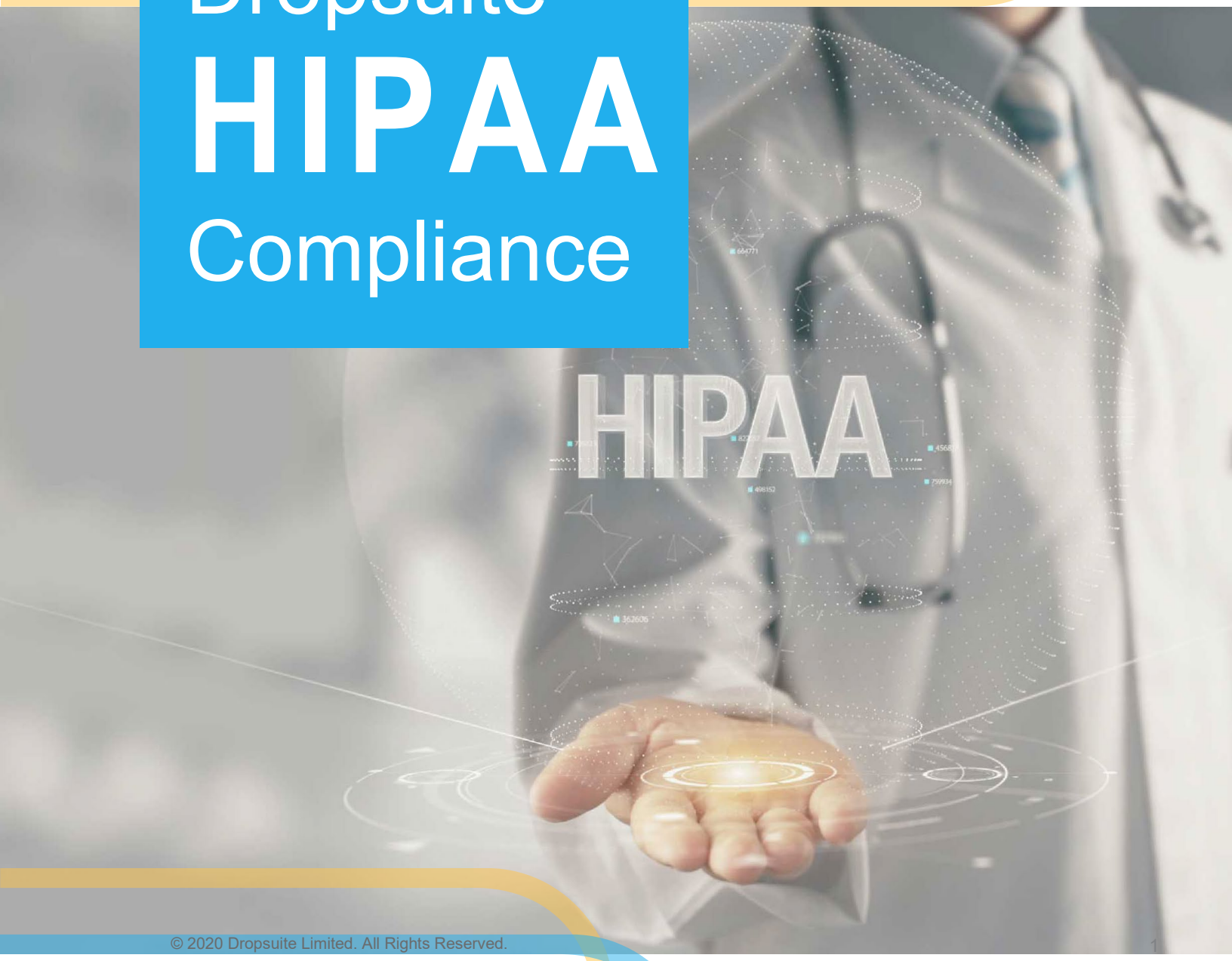
Dropsuite

Dropsuite HIPAA Compliance



© 2020 Dropsuite Limited. All Rights Reserved.

Overview



Dropsuite is a leading cloud backup platform on a mission to ensure that businesses never lose data again. Dropsuite's Email Archiving with Backup is a cloud-based email archiving and backup solution for businesses that need to comply with HIPAA data regulation requirements - while having their emails securely backed up and accessible.

When accidental or malicious data deletions occur, clients can restore their data swiftly with just a few clicks. Powerful advanced search tools enable clients to find critical information in their data no matter which system (Exchange Online, SharePoint, OneDrive and more) that data may be located in.

Dropsuite Email Archiving is Perfect For:

- Office 365 (Exchange Online, SharePoint, One Drive and more)
- Exchange Server 2007, 2010, 2013 & 2016
- IMAP and POP3 Protocol Email Systems
- G Suite Gmail

Key Archiving Features:

- Untampered and Continuous Data backup
- Audit Logs
- Customizable Data Retention
- eDiscovery / Advanced Search
- Legal Hold
- Granular Reviews, Roles and Access Control

© 2020 Dropsuite Limited. All Rights Reserved.

HIPAA and Email Archiving



In the U.S., organizations that create, maintain, transmit, use and/or disclose Protected Health Information (PHI) or Electronic Protected Health Information (ePHI), are required to meet and comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). These organizations are named as Covered Entities or Business Associates of Covered Entities.

Covered Entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Generally, the transactions concern billing and payment for services or insurance coverage. For example, hospitals, academic medical centres, physicians, and other health care providers who electronically transmit claims transaction information directly or through an intermediary to a health plan are Covered Entities. Covered Entities can be institutions, organizations, or persons.

Business Associate is defined as a person or entity who, on behalf of a Covered Entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information such as; data analysis, claims processing or administration, utilization review, quality assurance reviews, or any other function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule.

Business associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management,

© 2020 Dropsuite Limited. All Rights Reserved.

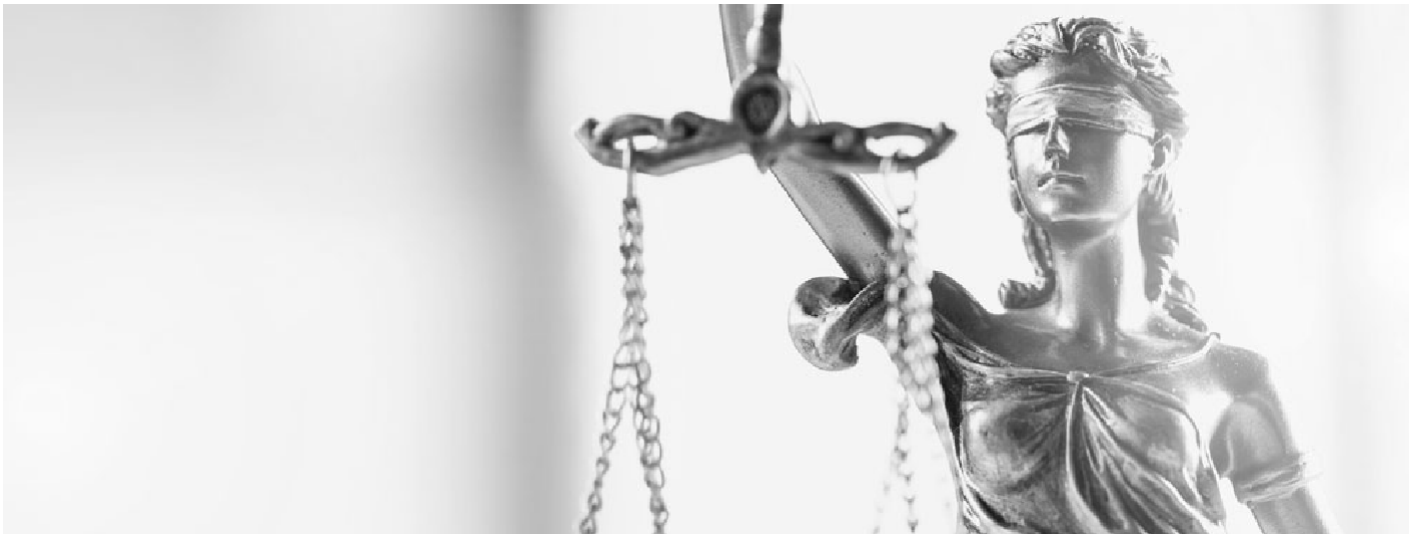
administrative, accreditation, or financial services to or for a Covered Entity where performing those services involves disclosure of individually identifiable health information by the Covered Entity or another business associate of the Covered Entity to that person or entity. A member of a Covered Entity's workforce is not one of its business associates. A Covered Entity may be a business associate of another Covered Entity.

While Dropsuite is not a Covered Entity, we are a Business Associate of a Covered Entity that uses our service under HIPAA. We offer an email archiving solution to healthcare providers who are Covered Entities and need to be fully HIPAA compliant. In order to ensure that our healthcare customers meet HIPAA requirements, Dropsuite's email archiving solution is HIPAA Privacy Rule and Security Rule compliant.

Dropsuite's email archiving solution is HIPAA Privacy Rule and Security Rule compliant.

© 2020 Dropsuite Limited. All Rights Reserved.

HIPAA Privacy Rule



The Privacy Rule applies to health plans, healthcare clearinghouses, and any health care provider that transmits health information in electronic form in connection with transactions regulated by HHS (“Covered Entities”).

Dropsuite implements reasonable safeguards for data that is archived with our solution to prevent any intentional or unintentional use or disclosure that is in violation of the requirements of HIPAA for clients that are regulated by the Department of Health and Human Services (HHS).

Dropsuite employs role-based access control to our archiving solution so end clients or their outsourced IT provider can control access levels to users.

- Individuals can only access their own data
- Administrators have data recovery and eDiscovery access only
- Two factor authentication ensures only authorized users can login
- Audit logs track and record all access and changes

© 2020 Dropsuite Limited. All Rights Reserved.

HIPAA Security Rule



The HIPAA Security Rule requires appropriate Technical, Physical, and Administrative Safeguards to ensure the confidentiality, integrity, and security of protected health information (PHI).

Three Parts to the Security Rule:

- Technical Safeguards
- Physical Safeguards
- Administrative Safeguards

TECHNICAL SAFEGUARDS

End to end security

Dropsuite's solutions use Transport Layer Security (TLS 1.2) cipher for all incoming and outgoing data traffic. Data at rest is stored on our Amazon Web Services (AWS) infrastructure and encrypted with military-grade 256-bit Advanced Encryption Standard (AES256). Our end to end encryption ensures that data in transit and at rest is safe and secure.

User access control

The default user access control in Dropsuite is "No Privilege.' Employees and users in Dropsuite will only have access to what is needed, when it is needed. Employees will only be granted access to

© 2020 Dropsuite Limited. All Rights Reserved.

internal systems based upon their work requirements. Requests for additional access follows a documented process and are approved by the responsible owner or manager.

Access to the production systems will be through a secured VPN tunnel that only authorized developers will have access to. Further access to individual AWS regions will require Two-Factor Authentication to prevent internal identity theft. Furthermore, clients' internal IT administrator or outsourced IT service providers will not have access to the content of the emails without an end client explicitly granting permission.

Audit Logs

Dropsuite tracks and logs every server, router, system call, command procedure and more of our production environment. All activities performed by users are tracked and can be retrieved for audit purposes. Logs are kept for 7 years as required by HIPAA, to ensure our systems are secure.

PHYSICAL SAFEGUARDS

Data Center

Dropsuite does not store any PHI/ePHI data on our premises. All data is stored with our infrastructure service provider (AWS). All AWS data centers are SAS 700II certified and comply with HIPAA Privacy and Security Rules.

Workspace Access

All physical access to Dropsuite's offices and workspace is secured with biometric devices and all visitors are required to be escorted at all times.

Data Disposal

Upon ending the subscription to Dropsuite's email archiving solution, data will be permanently deleted after 30 days and not retrievable by any means.

© 2020 Dropsuite Limited. All Rights Reserved.

ADMINISTRATIVE SAFEGUARDS

Vulnerability Testing

Dropsuite engages independent external entities to conduct regular application-level and infrastructure-level vulnerability tests. We also continue to scan and test the Dropsuite application internally, and on a regular basis, preforming regular security patches or upgrades. Results of the external vulnerability testing and remediation are shared by the entire team including management and the board of directors.

Personnel Management

All employees are required to complete an internal data privacy and security training annually. All developers go through yearly training in data privacy and security. Individuals with elevated levels of access are required to take a biennial HIPAA certification with a private provider. Employees are required to report security and privacy issues to our Data Protection Officer. Employees are informed that failure to comply with acknowledged policies may result in consequences, up to and including termination. Furthermore, all employees sign confidentiality agreements upon joining the company.

HIPAA Security and Privacy Officers

Dropsuite has appointed several HIPAA Security and Privacy officers and all our officers have completed HIPAA certification.

© 2020 Dropsuite Limited. All Rights Reserved.

HIPAA Breach Notification Rule



The Breach Notification Rule requires HIPAA Covered Entities and their business associates to prove notification to HHS following a breach of unsecured PHI. In the event the breach affects more than 500 patients, notification must also be provided to the media and public.

Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third-party service providers, pursuant to Section 13407 of the HITECH Act.

Covered Entities and Business Associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a Covered Entity (or Business Associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required.

Dropsuite is considered as a Business Associate of any Covered Entity that uses our service under the HIPAA and HITECH Act. In order ensure that our clients' data are secure and to provide timely notification in the unlikely event of a data breach, Dropsuite has a Breach Notification Plan in place to Contain, Notify, Evaluate and Respond in the event of a data breach.

© 2020 Dropsuite Limited. All Rights Reserved.

HIPAA Enforcement Rule



The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

To facilitate the compliance with the HIPAA Enforcement Rule, Dropsuite has built in the following features:

- Customizable retention period (1-10 years or forever)
- eDiscovery and Advanced Search
- Legal Hold

HIPAA regulates that all ePHI should be retained for 7 years, after which the data should be immediately deleted unless there is a legal reason to keep it. The super admin can set the retention period within the Dropsuite Email Archiving control panel, and the system will automatically delete any data once it has passed the 7 year retention requirement.

In the event of a violation enforcement or civil litigation, eDiscovery provides comprehensive and easy search capabilities to discover the required data. All required data can then be put on legal hold, so it cannot be deleted, until the litigation is over and the admin removes the legal hold.

© 2020 Dropsuite Limited. All Rights Reserved.