BooleBox - Getting started with HIPAA

Follow our Best Practices to understand how to configure your BooleBox account in order to meet your responsibilities under HIPAA and ensure the privacy of confidential medical information

HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by U.S. Congress in 1996. The HIPAA Privacy regulations require health care providers and organizations, as well as their business associates, to develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared.

In this document you will find a few recommended best practices that customers subject to HIPAA should consider when configuring their BooleBox accounts, to make sure their use is consistent with the above mentioned legal requirements.

Grant maximum protection to data access

BooleBox gives you complete privacy and 360° control over sensitive data.

Besides keeping Protected Health Information (PHI) secure in a protected storage, you can easily share it with extreme flexibility with both internal and external users.

Depending on your needs, you can apply advanced security settings when sharing single files, entire folders or even messages with extreme granularity. In this way, you can be sure that the most sensitive data do not fall prey of unauthorized users, while at the same time maintaining real-time visibility and full control over all sharing activities.

Classify data in a controlled way

BooleBox guarantees optimum protection of shared data with default file classification according to preset encryption rules and access authorization established by the administration.

Sensitive data will be automatically protected and made accessible in a selective and granular manner, responding to business needs and respecting company security policies. This entails the promotion of the so called “Security culture”: more responsible users handling sensitive data.

Secure authentication procedures

To further secure the login phase, team admins can require members use *two-step verification* to sign in to their BooleBox accounts. Once enabled, BooleBox will require a six-digit security code in addition to a password upon sign-in or when linking a new device. This highly recommended security feature adds an extra layer of protection to users accounts.

Furthermore, thanks to *Single sign-on* (SSO), BooleBox users will be able to use one set of login credentials to access multiple applications: the service, indeed, authenticates users for all the applications they have been given rights to and eliminates further prompts when they switch applications during the same session.

Configure users settings and supervise corporate accounts

Thanks to BooleBox dashboard, admins have full control over company corporate accounts. BooleBox control panel, indeed, offers a summary view of all BooleBox users within the team, and admins have the possibility to manage their settings – such as storage space and security parameters. Team members can be easily added, removed and reviewed. For instance, admins can remove access when employees leave the company or no longer require access due to a change in job role.

Furthermore, thanks to *BooleBox AD Sync*, BooleBox administrators can perform automatic user provisioning from their existing Active Directory System and manage their work groups directly from their account in a simple and quick way.

Monitor users activities

A great added-value of BooleBox is its advanced auditing system, which contains detailed information about *who* has accessed corporate confidential files, *what* operations have been performed, *when* and *where*. As a team admin, you can view and export these auditing reports to know in detail your team's sharing, authentication and editing activities.

It is fundamental to regularly review audit logs to keep an eye out for any unusual activity – access from unauthorized devices, unauthorized editing activities, … –, help maintain your sensitive information totally secure and ensure compliance with requirements.

Disable permanent file deletion

BooleBox users have the possibility to access their files version history, where they can find all the previously modified versions of their projects, presentations and spreadsheet. At the same time, they have the chance to recover files and folders that were previously deleted, unless a user requests a permanent deletion or a team admin closes the account.

To help customers adhere to HIPAA requirements, we suggest admins disable the "Empty Recycle Bin" functionality from the dashboard. In this way, you can retain team members' documents containing highly confidential data for the lifetime of your account, for a permanent, 360° control.

Keep an eye on third-party apps and integrations

BooleBox can count on a strong network of third-party apps and integrations, thanks to which your account can gain added functionality in terms of both collaboration and security.

Advanced tools that can be great complements to your account, even strengthening your existing security practices. Having said that, it is also extremely important to remember that they're not part of BooleBox included services: for this reason, we recommend that you always assess them and make sure that they respect all regulatory requirements. Total, preventive control, for better collaboration and results.

Entrust secure data location for your cloud

Sometimes, it is essential for customers who operate in highly regulated industries or in countries with strict data protection laws to know the geographic location of the data that they have entrusted to our cloud service.

If you have opted for BooleBox Cloud secure collaboration platform, you know exactly where your data is stored. BooleBox Cloud customer data is replicated within a selected geographic area for enhanced data durability in case of a major datacenter disaster. We also understand that some customers must maintain their data in a specific geographic area. We rely our services on the highly guaranteed provider, Amazon Web Services (AWS). To satisfy the need of maintaining data in Europe, we chose Ireland as our storage and Germany as location where to replicate it. In detail, Amazon S3 Bucket is used as Object Storage Unit, while Amazon RDS as Database. BooleBox Cloud platform therefore inherits every single characteristic from Amazon S3 infrastructure SLA*.

* Amazon S3 Service Level Agreement, https://aws.amazon.com/s3/sla/