Google Cloud

HIPAA Compliance with G Suite

G Suite HIPAA Implementation Guide

Google Cloud

Table of Contents

Google works to keep users' data secure in the cloud in a reliable, compliant way.

The combination of security and privacy lead to a strong ecosystem that keeps your information safe. For customers who are subject to the requirements of the Health Insurance Portability and Accountability Act (known as HIPAA, as amended, including by the Health Information Technology for Economic and Clinical Health — HITECH — Act), G Suite supports HIPAA compliance.

This guide is intended for security officers, compliance officers, IT administrators, and other employees in organizations who are responsible for HIPAA implementation and compliance with G Suite. Under HIPAA, certain information about a person's health or health care services is classified as Protected Health Information (PHI). After reading this guide, you will understand how to organize your data on Google services when handling PHI to help meet your compliance needs.

Customer Responsibilities

Customers are responsible for determining if they are a Business Associate (and whether a HIPAA Business Associate Agreement (BAA) with Google is required) and for ensuring that they use Google services in compliance with HIPAA. Customers are responsible for fulfilling an individual's right of access, amendment, and accounting in accordance with the requirements under HIPAA.

Using Google Services with PHI

G Suite customers who are subject to HIPAA and wish to use G Suite with PHI must sign a G Suite Business Associate Agreement (BAA) with Google. Per the G Suite BAA, PHI is allowed only in a subset of Google services. These Google covered services, which are "Included Functionality" under the HIPAA BAA, must be configured by IT administrators to help ensure that PHI is properly protected. In order to understand how the Included Functionality can be used in conjunction with PHI, we've divided the G Suite Core Services ("Core Services") covered by your G Suite Agreement into three categories. G Suite administrators can limit which services are available to different groups of end users, depending on whether particular end users will use services with PHI.

1. **HIPAA Included Functionality: All users can access this subset of Core Services for use with PHI under the G Suite BAA as long as the health care organization configures those services to be HIPAA compliant: Gmail, Calendar, Drive (including Docs, Sheets, Slides, and Forms), Apps Script, Keep, Sites, Jamboard, Hangouts (chat messaging feature only), Hangouts Meet, Google Cloud Search, and Vault (see full list of G Suite Core Services here).**

2. **Core Services where PHI is *not* permitted: Any Core Service not listed in section 1 may not be used connection with PHI. G Suite administrators can choose to turn on these remaining Core Services[1], which may include Contacts, Groups, and Google+ , for its users, but it is their responsibility to not store or manage PHI in those services. It is possible that the list of Core Services may be updated from time to time. Any updates to such functionality should be considered by default to be included in this category unless expressly added to the definition of Included Functionality. Please see "Separating user access within your domain" for further details on how to utilize organizational units to manage user access to services that are appropriate for PHI.**

Core Services in which PHI is permitted
Gmail
Calendar
Drive (including Docs, Sheets, Slides, and Forms)
Apps Script
Keep
Sites
Jamboard
Hangouts (chat messaging feature only)
Hangouts Meet
Google Cloud Search
Vault (if applicable)

[1]Core Services are dependent on which version of G Suite a customer has purchased as described in the applicable services summary

Core Services in which PHI is not permitted
Google Groups
Google Contacts
Google+

3. Other Non-Core Services Offered by Google: PHI is *not* permitted in other Non-Core Services offered by Google where Google has not made a separate HIPAA BAA available for use of such service. All other Non-Core Services not covered by your G Suite Agreement, including, for example, (without limitation) YouTube, Blogger and Google Photos (see list of Additional Google Services here), must be disabled for G Suite users who manage PHI within the Included Functionality - unless covered by a separate BAA. Only users who do not use Included Functionality to manage PHI may use those separate Non-Core Services offered by Google (under the separate terms applicable to these Google services). Please see "Separating user access within your domain" for further details on how to utilize organizational units to restrict access to services that are not HIPAA compliant.

4. Technical Support Services: Technical support services provided to Customer by Google are not part of the HIPAA Included Functionality. Customers should not provide PHI to Google when accessing technical support services.

To manage end user access to different sets of Google services, G Suite administrators can create organizational units to put end users who manage PHI and end users who do not into separate groups. Once these units are set up, an administrator can turn specific services on or off for groups of users. Those who manage PHI, for instance, should have non-Core Services turned off. Please see "Separating user access within your domain" in the "Additional Considerations for HIPAA Compliance" section below for further details on how to utilize organizational units.

To learn more about how Google secures your data, please review our G Suite security whitepaper.

What to Consider for Specific G Suite Core Services

Every G Suite Core Service has specific settings to adjust to help ensure that data is secure, used, and accessed only in accordance with your requirements. Here are some actionable

recommendations to help you address specific concerns within services that are HIPAA Included Functionality:

Monitoring account activity

The Admin console reports and logs make it easy to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. To monitor logs and alerts, admins can configure notifications to send them alerts when Google detects these activities: suspicious login attempts, user suspended by an administrator, new user added, suspended user made active, user deleted, user's password changed by an administrator, user granted admin privilege, and user's admin privilege revoked. The admin can also review reports and logs on a regular basis to examine potential security risks. The main things to focus on are key trends in the highlights section, overall exposure to data breach in security, files created in apps usage activity, account activity, and audits.

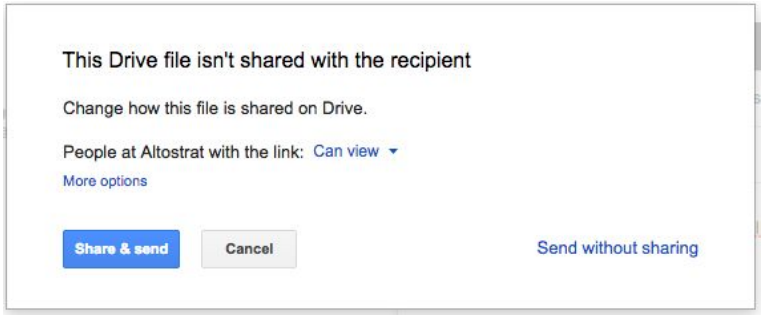
Search history

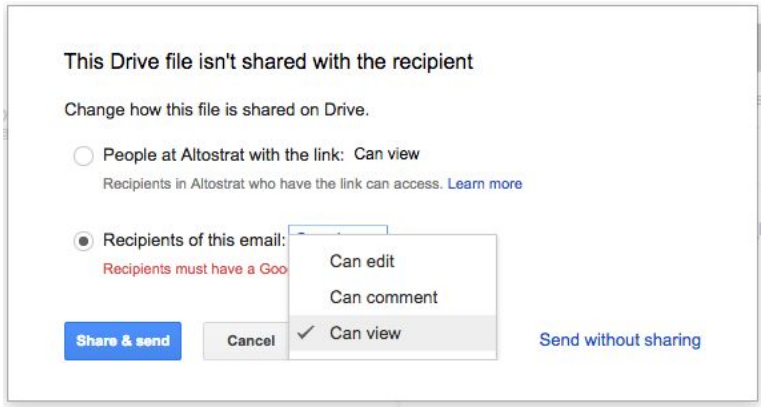
It is recommended to turn off search history for services where the search history may be accessed beyond the individual account.

Gmail

Gmail provides controls to ensure that messages and attachments are only shared with the intended recipients. When composing emails and inserting files using Google Drive that potentially contain PHI, end users can choose to share only with the intended recipients. If the file is not already shared with all email recipients, the default will be to share the file with "Anyone with the link" within the G Suite domain. Change the link sharing settings to "Private."

Please refer to the Use of third party applications for guidance on using third party applications with Gmail.

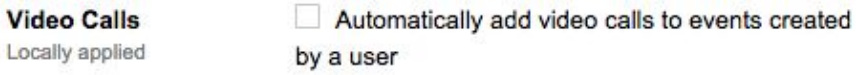




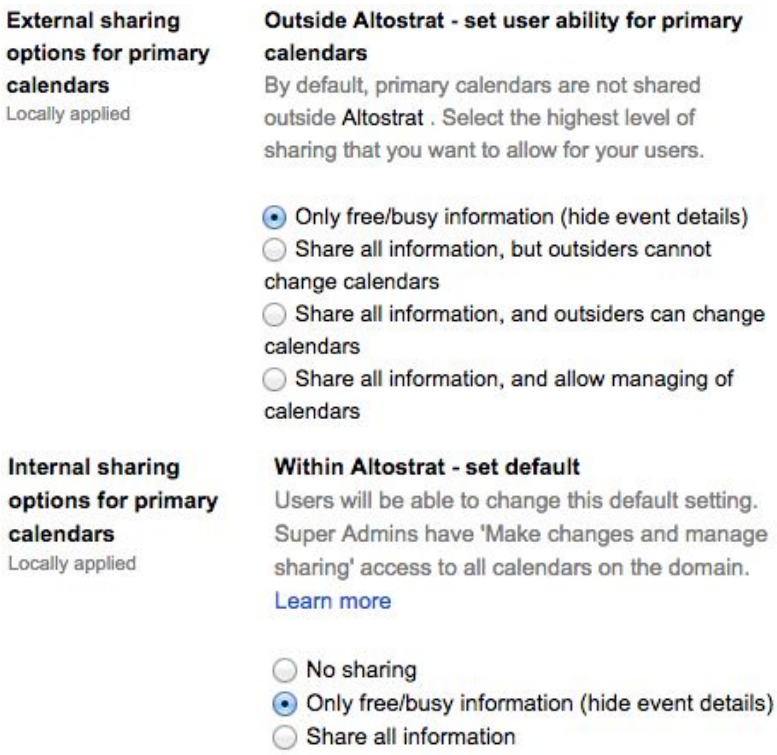
Calendar

Within your domain, employees can change if and how their calendar is shared. Admins can set sharing options for all calendars created in the domain. By default, all calendars share all information to anyone within your domain, and only free/busy information with all external parties. To limit exposure of PHI within the domain, employees should consider setting calendar entries to "Private" for calendar entries that contain PHI. Calendar provides a feature that can add a link to a Hangout video meeting to the Calendar entry. Please see details below regarding use of Hangouts for video meetings.

Admins should consider disabling the option to automatically add Hangout video calls to calendar event entries for employees who manage PHI.

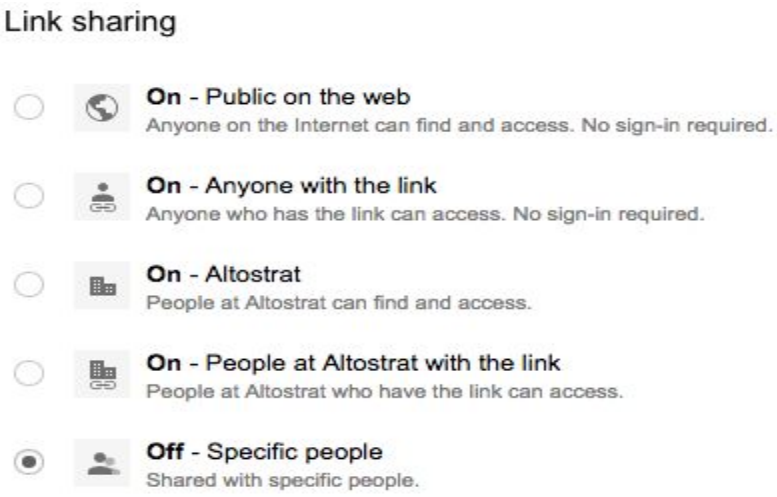


Admins should consider setting calendar sharing options to "No sharing" or "Only free/busy information" for employees who handle PHI.

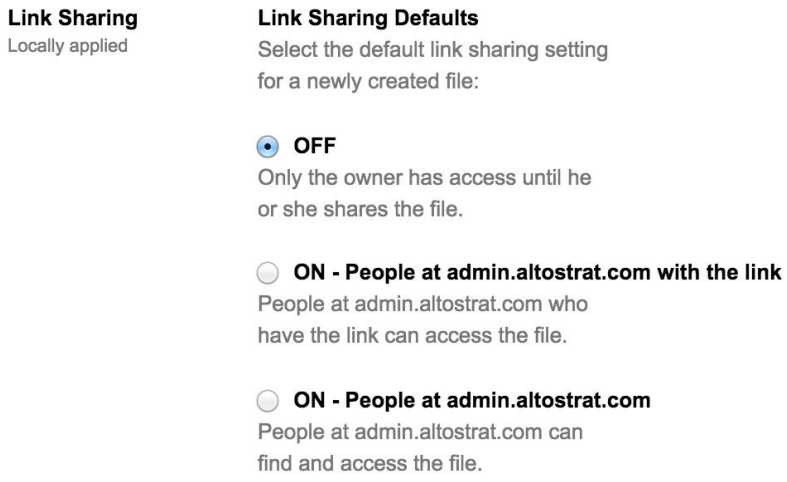


Drive (including Docs, Sheets, Slides, and Forms)

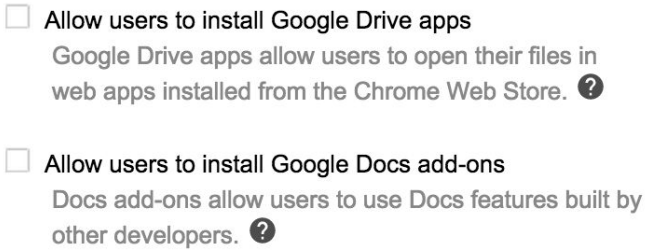
Employees can choose how visible files and folders are, as well as the editing and sharing capabilities of collaborators, when sharing files in Google Drive (including Docs, Sheets, Slides, and Forms). When creating and sharing files in Google Drive (including Docs, Sheets, Slides, and Forms) it is recommended that users avoid putting PHI in titles of such files, folders, or Team Drives.



Admins can set file sharing permissions to the appropriate visibility level for the G Suite account. Admins can "Restrict" or "Allow" employees to share documents outside the domain, and set the default file visibility to "Private." In particular, sharing settings also affect whether Team Drives in your domain may have external users as members, and whether your users may be members of Team Drives in other domains. For more on Team Drives, see this article.



Admins should consider disabling third party applications that can be installed, such as Google Drive apps and Google Docs add-ons. Admins should review the security of these applications, as well as any corresponding security documentation provided by the third party developer.



Apps Script

See the Drive section above for guidelines regarding how and with whom to share Apps Script projects. It is recommended that projects that access PHI should be accessible only by users who are permitted to access the PHI.

When using Apps Script to generate emails or other messages, to update Docs, Sheets or other documents, or to send data to another application, ensure that PHI is included only if all recipients or users with access to the target file or system are authorized to access it.

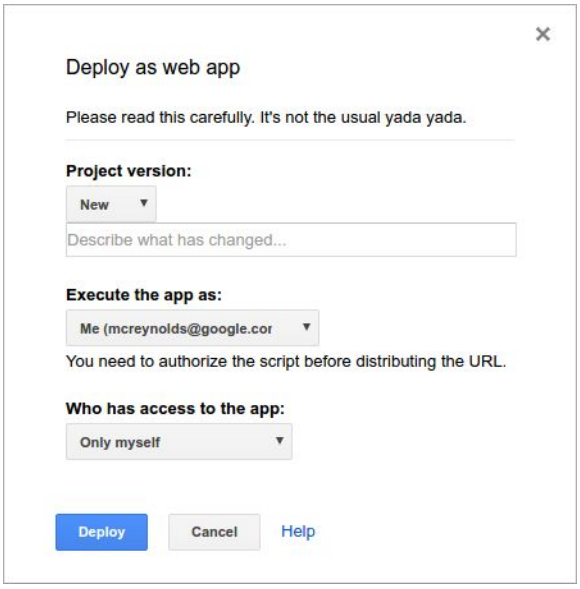
When using ScriptProperties, DocumentProperties or any other shared data store, do not store PHI unless your Apps Script project and any deployments are accessible only to users who are allowed to access the stored PHI.

When using the JDBC or UrlFetchApp service, do not insert PHI into an external database or upload it to an external web service unless the database or web service is only accessible to users who are authorized to access PHI. Do not use JDBC or UrlFetchApp to insert or upload PHI to Google Cloud Platform services and APIs, and do not use the `console.*` functions to log PHI to Stackdriver Logging, without signing a BAA with Google Cloud Platform.

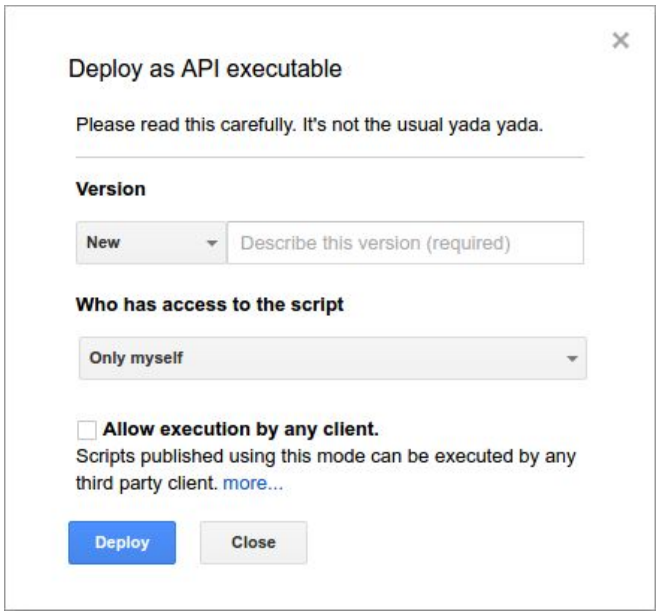
When using Apps Script is is recommended that access is limited to the minimum necessary to ensure that the code prevents unauthorized access to PHI. Below are some recommended configuration settings for particular use cases.

When deploying an Apps Script project that handles PHI as a web app, under “Execute the app as,”it is recommended to select “User accessing the web app.”

If the web app needs to execute as you, under “Who has access to the app,” select “Only myself.” If the web app needs to execute as you and other users need to have access, select “Anyone within [your domain]” and ensure that your code blocks any user who should not have access to PHI.

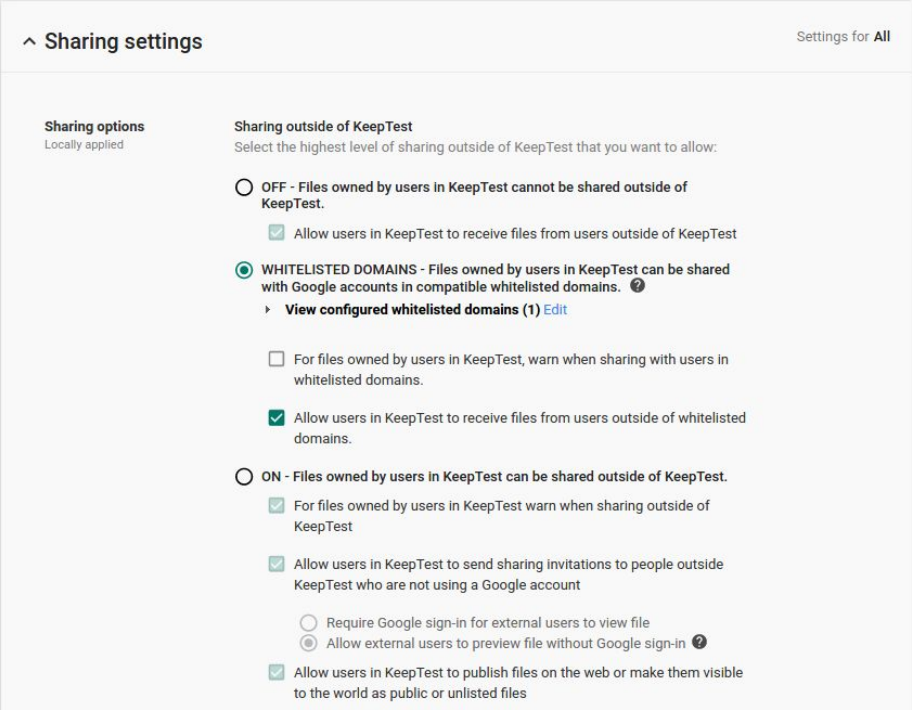


When deploying an Apps Script project as an API executable, under "Who has access to the script," select "Only myself." Or, if other users need to have access, select "Anyone within [your domain" and ensure that your code blocks any user who should not have access to PHI.

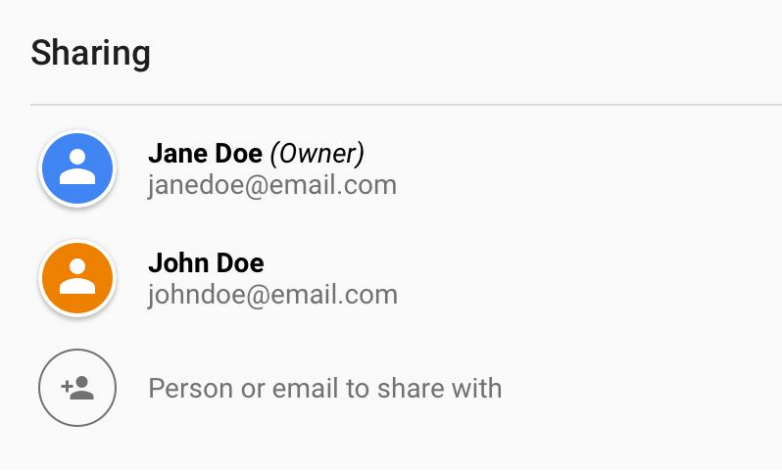


Keep

In Drive sharing settings, Admins can set file sharing permissions to the appropriate visibility level for the G Suite account. Admins can "Restrict" or "Allow" employees to share documents outside the domain, and set the default file visibility to "Private."



The sharing settings for notes created in Google Keep are a sub-set of Drive sharing settings, however all Keep notes created by employees have a default visibility set to "Private" regardless of the Drive settings.



Keep does not support a concept of "Public" notes, or notes visible to those with the URL. Instead, employees can choose to add collaborators to individual Keep notes via individual email addresses or group aliases. All collaborators added to a note have full access to view and edit the contents of a note (e.g. content in the title, body and list of the note, in addition to any attached images, drawings, or audio).

Employees can color, label, add reminders, and archive their notes, however these note attributes are per user, and are not shared with other note collaborators. The original owner of a note has the option to Trash the note, which will trash the note for all collaborators as well. Collaborators on a note are not able to Trash the note, however they can choose to unsubscribe from the note if they choose.

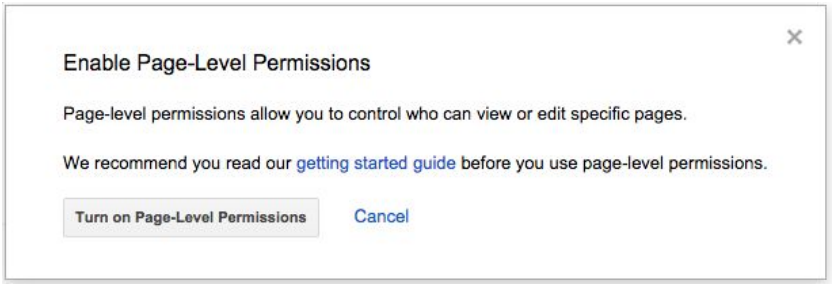
Sites

The Sites service (both classic and new versions), like all G Suite Core Services, does not serve advertising or use customer data for advertising purposes, however, some legacy users of AdSense on the classic version of Sites may retain the ability to use the separate AdSense product to display advertising on their Sites pages. Users should ensure that AdSense on the classic version of Sites is disabled whenever the classic version of Sites is used with PHI.

For sites containing PHI, employees should configure the sharing and visibility settings appropriately. Instructions to configure these settings are outlined below separately for each version of Sites (classic and new):

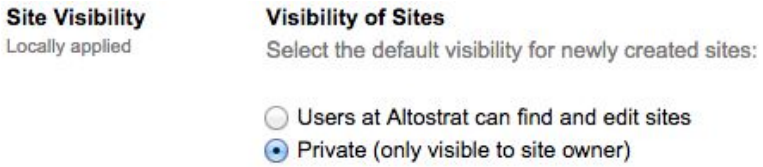
Sites (classic version)

Employees can set the sharing settings for sites created in classic Sites to control who can edit or view their sites. Employees can also turn on page-level permissions to granularly control who has access to individual web pages within a site.



Employees should set the sharing permissions appropriately, if inserting a Google Calendar or content stored in Google Drive (including Docs, Sheets, Slides, and Forms) into a site.

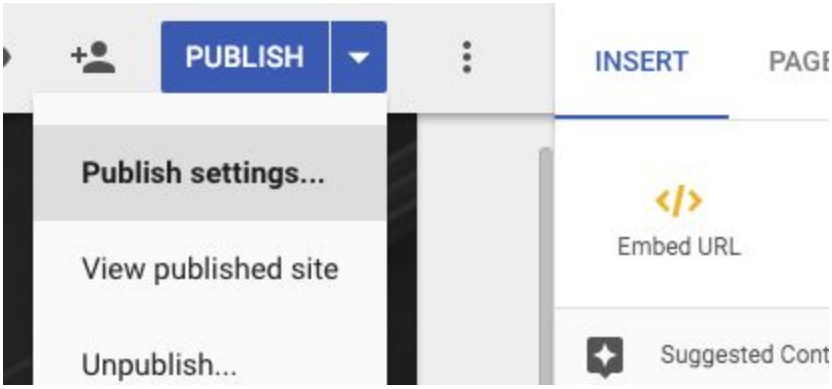
Admins should consider setting the default visibility for sites to "Private."



Sites (new version)

The new version of Sites relies on a combination of Sites and Drive settings. Admins can allow (or disallow) employees to create and edit sites using new Sites, using a control for this purpose located under the Sites icon in the Admin console. Admins control the level of sharing and visibility allowed for sites created in new Sites using the sharing settings for Drive in the Admin console.

For sites containing PHI, employees should consider giving limited editing access to specific individuals. Employees should also consider not publishing their site to outside their domain.



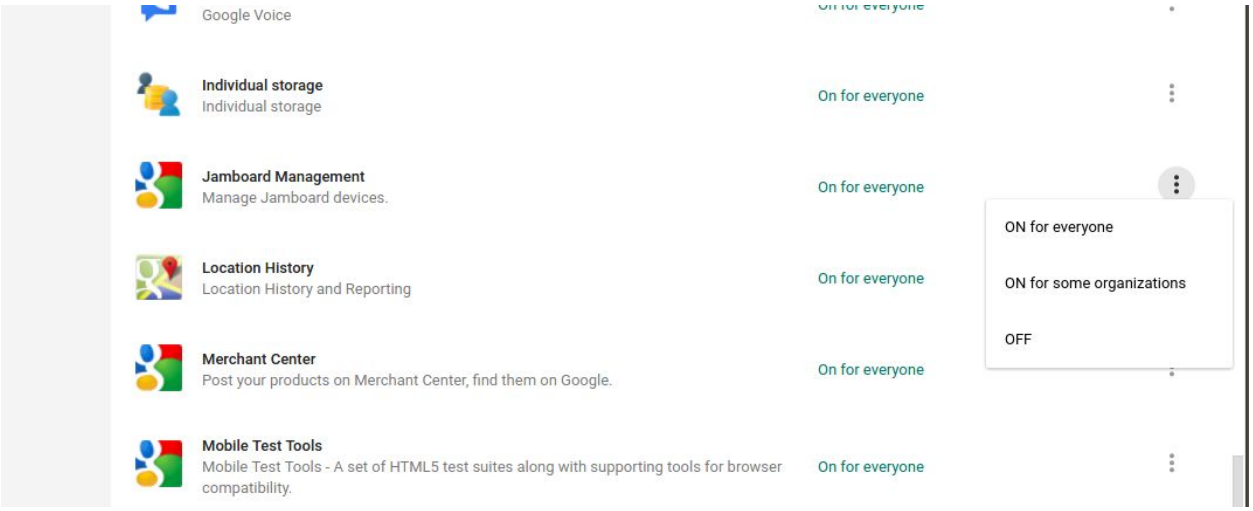
Employees should set the sharing settings for sites appropriately if inserting text, images, or other content (such as a Google Calendar or content stored in Google Drive (including Docs, Sheets, Slides, and Forms)) into a site.

Jamboard

Jamboard is the hardware device built for collaborative whiteboarding. The software application running on the kiosk, tablets and phone is also called Jamboard. Documents hosted on any of the above devices are called Jams.

Administrators can configure settings for Jamboard within the CPanel. The Jamboard app has a service on/off switch in CPanel, shown below. This is where an admin can turn off the service if they wish to.

For more information, please refer to Turn on the Jamboard service for your users support article.



Only the active Jam session is also stored locally on a device. Once a new Jam has been started the previous Jam document will be deleted from the device.

Sharing Settings

In Drive sharing settings, Admins can set file sharing permissions to the appropriate visibility level for the G Suite account. Admins can "Restrict" or "Allow" employees to share documents outside the domain, and set the default file visibility to "Private." The sharing settings for Jam files are a sub-set of Drive sharing settings.

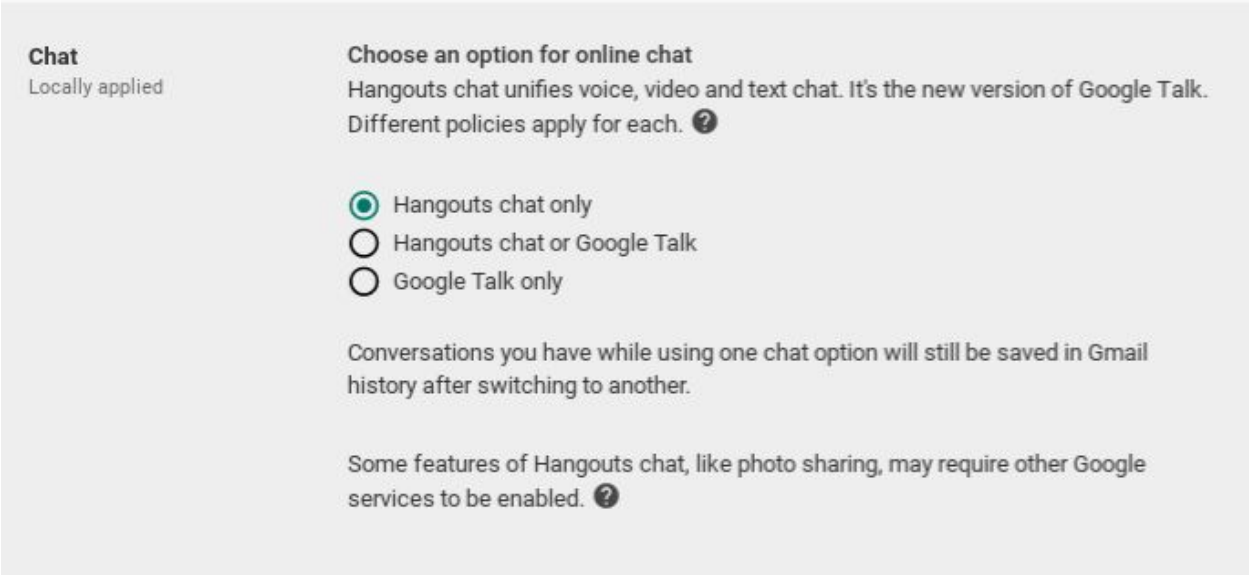
For more information on how to use the Jamboard to create, host, and edit Jams, refer to Working in a live Jam session support article.

Jam files created on a board will initially be owned by the board account. Once a user claims a file from the board, ownership will be transferred to the user, and the board will appear in the "Who has access" list as a collaborator (see image above for reference). Only users within the same domain as the board can claim Jam files from the board.

The original owner of a Jam file has the option to trash the Jam, which will trash the Jam for all collaborators as well. Collaborators on a Jam file can trash the file, which will only remove the Jam file from their Jam list. It will not trash the Jam for any other collaborator on the file.

Hangouts (chat messaging feature only)

Admins should configure Hangouts Chat in their domain to the "Hangouts chat only" setting as shown below.



It is recommended that users start a new chat when adding multiple members to a chat conversation. Additionally, users should refrain from using PHI in group chat naming. New members that are added to group chats will be able to see previous chat history.

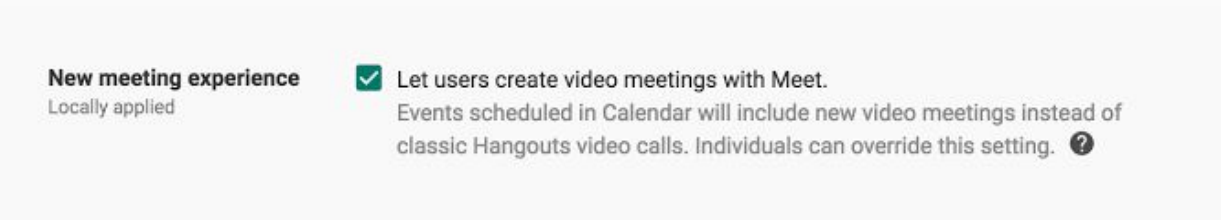
Admins can control whether their users can chat with others outside of their organization, display users' chat status outside of their organization, or warn users when they are chatting with others outside of their organization.

Additionally users can control whether others inside or outside of their organization can see when they were last seen online, which device they are on, and when they are in a video or phone call on their devices.

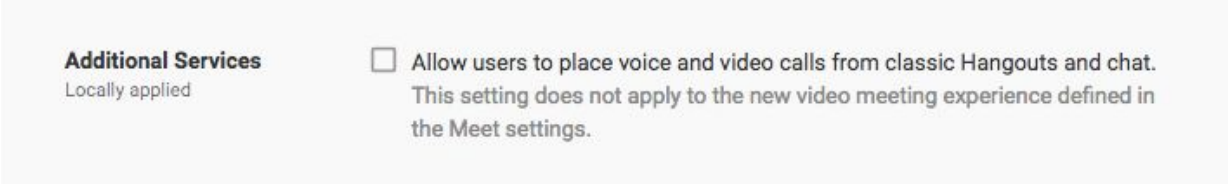
Admins should configure these settings consistent with the organization's policies.

Hangouts Meet (Hangouts new video meeting experience)

Meet, the new video meeting experience from Hangouts, allows for HIPAA compliant use. In order to configure and use Meet, please ensure the checkbox below is selected in the Hangouts administrator settings. Enabling Meet will cause Google Calendar to offer this type of video meeting instead of classic Hangouts named video calls.



Unlike Meet, classic Hangouts named video calls are not covered by G Suite's HIPAA Business Associate agreement. To prevent users from starting video calls from classic Hangouts, uncheck the box below to disable this functionality.



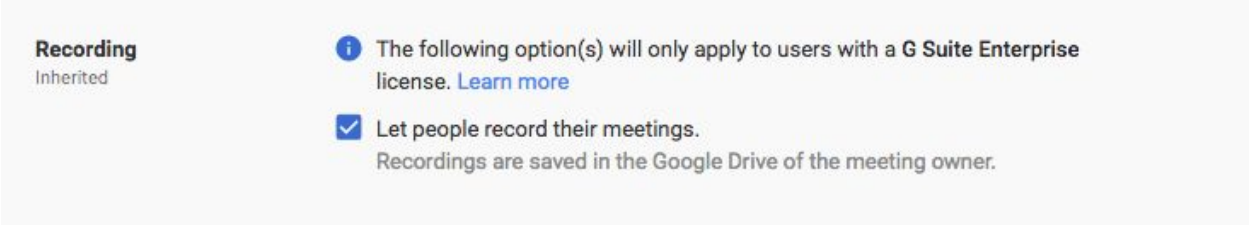
Meet allows you to control whether external guests may participate in each video meeting. People in the same domain can manage external guest access by controlling who gets invited to the meeting, determining whether to permit anonymous guests to join a running video call, and removing unwanted participants from the call. Please see the Hangouts support pages for more information on inviting guests.

Meet uses randomized meeting identifiers and dial-in details. It is not possible to customize external access identifiers to video meetings so there is no need to randomize any addressing information.

Meet meetings allow for users to share text-based chat messages with other participants. Messages are only available during the call.

Meet allows users to record meetings which are then saved to the Drive of the meeting owner. The recording is saved in MP4 format and is a regular file in Drive with all Drive controls available, including Vault policies. The recording is automatically shared with guests invited to the Calendar event. Chat messages sent during a recorded call are preserved as a .txt file alongside the recording.

Admins are able to control whether users can record their meetings in the Admin console.



Google Cloud Search

Admins can control the use of search history with Google Cloud Search via the Web History service in the Admin console. Admins can turn the Web History service on or off for everyone, or for select organizational units. Users with Web History turned on will have their personal search history stored, and will benefit from better search results and suggestions. Search history is stored until deleted by a user at history.google.com.

For more information about Cloud Search, please see https://support.google.com/cloudsearch.

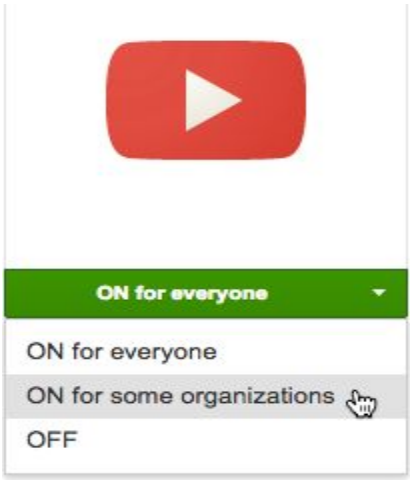
Additional Considerations for HIPAA Compliance

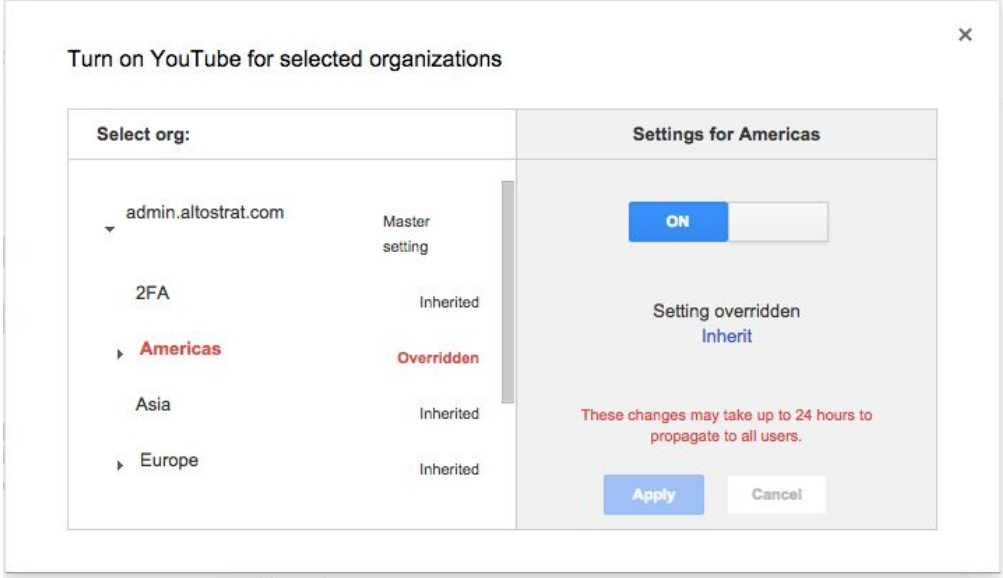
Separating user access within your domain

To manage end user access to different sets of Google services, a G Suite administrator can create organizational units to put end users who manage PHI and end users who do not into separate groups. Once these units are set up, the administrator can turn specific services on or off for groups of users.

In a small G Suite account, for instance, there are typically two or three organizational units. The largest unit includes employees with most services enabled, including YouTube and Google+; another unit is for employees who may manage PHI, with certain services disabled. In a more complex G Suite account, there are more organizational units that are often divided by department. Human resources may manage PHI, but those who do may be only a subset of HR employees. In that case, administrators could configure an HR organizational unit with most services enabled for some users, and another HR organizational unit for employees using the HIPAA Included Functionality with PHI (with certain services disabled and settings configured appropriately).

To learn more, please refer to our Support resources that discuss how to set up organizational units and how to turn services on and off.





Use of third party applications

If an end user wants to use the HIPAA Included Functionality to share PHI with a third party (or a third party application), some of the services may make it technically possible to do so. However, it is the customer's responsibility to ensure that appropriate HIPAA-compliant measures are in place with any third party (or third party application) before sharing or transmitting PHI. Customers are solely responsible for determining if they require a BAA or any other data protection terms in place with a third party before sharing PHI with the third party using G Suite services or applications that integrate with them.

To learn more, please refer to our Support resources that discuss how to control user installation of Marketplace apps.

Security best practices

To keep your data safe and secure, we recommend several security best practices including:

- **Set up 2-step verification to reduce the risk of unauthorized access in case a user's password is compromised**
- **Configure enterprise sender identity technologies — sender policy framework, DomainKeys Identified Mail, and Domain-Based Message Authentication — to prevent spammers and phishers from "spoofing" your domain**

Security Audits and Certifications

A list of security and privacy controls available with G Suite can be found on our Security and Privacy website.

In addition to supporting HIPAA compliance, the G Suite Core Services are audited using industry standards such as ISO 27001, ISO 27017, ISO 27018, and SOC 2 and SOC 3 Type II audits, which are the most widely recognized, internationally accepted independent security compliance audits. To make it easier for everyone to verify our security, we've published our ISO 27001 certificate and SOC3 audit report on our Google Enterprise security page.

Additional Resources

These additional resources may help you understand how Google services are designed with privacy, confidentiality, integrity, and availability of data in mind.

- G Suite Help Center
- G Suite security page
- HIPAA Compliance with G Suite

This HIPAA implementation guide is for informational purposes only. Google does not intend the information or recommendations in this guide to constitute legal advice. Each customer should independently evaluate its own particular use of the services as appropriate to support its legal compliance obligations.