Google Workspace and Cloud Identity

HIPAA Implementation Guide

The information contained herein is intended to outline general product direction and should not be relied upon in making purchasing decisions nor shall it be used to trade in the securities of Alphabet Inc. The information presented is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Any references to the development, release, and timing of any features or functionality described for these services remains at Google's sole discretion. Product capabilities, time frames and

features are subject to change and should not be viewed as Google commitments.

Table of Contents

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

Using Google services with PHI

What to consider for specific Google Workspace Core Services

- Monitoring account activity
- Search history
- Gmail
- Calendar
- Drive (including Docs, Sheets, Slides, and Forms)
- Data Studio
- Apps script
- Keep
- Sites
  - Sites
  - Sharing settings
- Google Chat
  - Sharing options
  - Bots and integrations
    - @Meet by Google
    - @Drive by Google
  - Third party apps and integrations
- Google Meet (Google's video meeting experience)
  - Meet Dialing to GV Users
- Google Cloud Search
- Cloud Identity Management
- Groups
- Google Voice (managed users only)
- Tasks
- Gemini in Workspace
- Gemini app as a Google Workspace Core Service (excluding Gemini in Chrome)
- Workspace Studio
- Separating user access within your domain
- Use of third party applications, systems, or databases
- Security best practices

Security audits and certifications

Additional resources

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

By combining the perspectives of both security and privacy, we help you keep 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), Google Workspace 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 Google Workspace and Google Cloud Identity. 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 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

Google Workspace customers who are subject to HIPAA and wish to use Google Workspace with PHI must sign a Business Associate Addendum (BAA) to their Google Workspace Agreement with Google. Google Cloud Identity customers who are subject to HIPAA and wish to use the services with PHI must sign a BAA to their Cloud Identity Agreement with Google. Per the Google Workspace and Cloud Identity 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 Google Workspace Core Services ("Core Services") and Cloud Identity services covered by your respective Agreements into three categories. 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 BAA as long as the health care organization configures those services to be HIPAA compliant:** Cloud Identity Management, Gemini app (excluding Gemini in Chrome), Gemini in Workspace, Gmail, Google Calendar, Google Chat, Google Cloud Search, Google Drive (including Google Docs, Google Forms, Google Sheets, Google Slides, and Google Vids), Google Groups, Google Keep, Google Meet, Google Sites, Google Tasks, Google Vault (if applicable), Google Voice (managed users only), and Google Workspace Studio. See full list of Google Workspace Core Services here. Users can follow the suggestions outlined in this implementation guide for guidance.

2. **Core Services where PHI is *not* permitted: Any Core Service not listed in section 1 may not be used in connection with PHI.** Google Workspace administrators can choose to turn on these remaining Core Services, which may include Contacts 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
Cloud Identity Management
Gemini app (excluding Gemini in Chrome)
Gemini in Workspace
Gmail
Google Calendar
Google Chat
Google Cloud Search
Google Drive (including Google Docs, Google Forms, Google Sheets, Google Slides, and Google Vids)
Google Groups

Google Keep
Google Meet
Google Sites
Google Tasks
Google Vault (if applicable)
Google Voice (managed users only)
Google Workspace Studio

Core Services in which PHI is not permitted
Google Contacts

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 Google Workspace Agreement, including, for example, (without limitation) YouTube, Blogger and Google Photos (see list of additional Google Services), must be disabled for Google Workspace 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.

5. **Pre-GA Offerings**: Do not use Pre-GA offerings (products or services offered under the Google Cloud Pre-General Availability Program or other pre-GA offerings as defined in Google's Service Specific Terms) in connection with PHI, unless expressly noted otherwise in a notice or other terms of the offering.

To manage end user access to different sets of Google services, Google Workspace

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 Trust and security page.

What to consider for specific Google Workspace Core Services

Every Google Workspace 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. Focus on key trends in the highlights section, overall exposure to data breach in security, files created in apps usage activity, account activity, and audits.

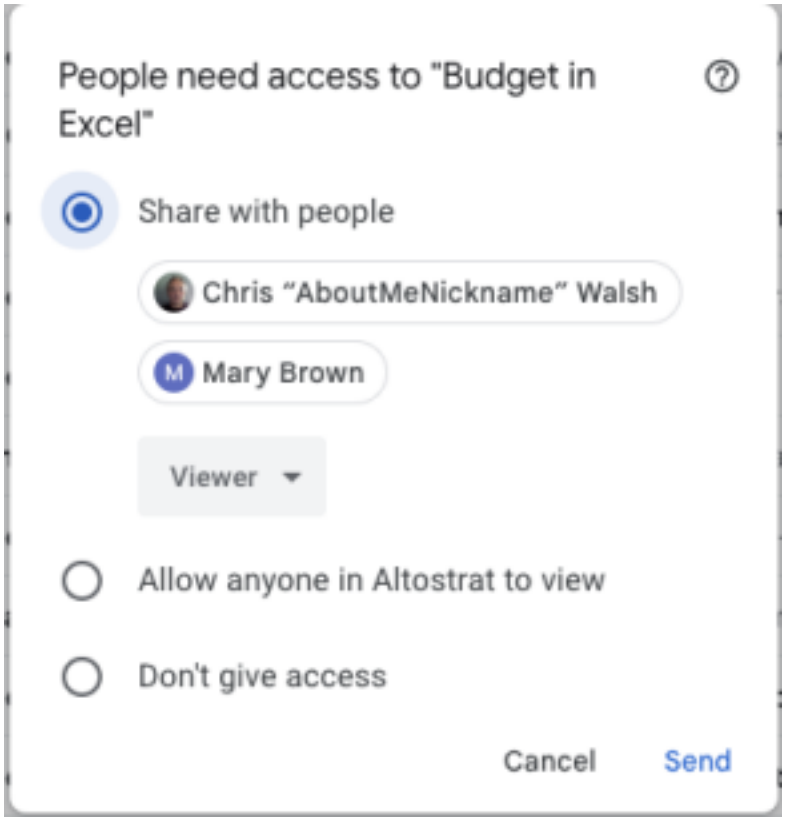
Search history

It is recommended to turn off search history for services where the search history may be accessed beyond the individual account. Following the principle of "minimally necessary", creating only the minimal amount of information needed to perform the function, this action reduces the amount of data collected and retained, reducing the burden of data protection. If it is not explicitly needed, don't collect it.

Gmail

Gmail provides controls to help users ensure that messages and attachments are only shared with the intended recipients. When composing emails and inserting files using Google Drive that may contain PHI, end users can choose to share only with the intended recipients. By

default, Drive Files that are being attached to Gmail are Restricted and sharing requires a subsequent action. If the file is not already shared with all email recipients, the Sender can choose to share the file with "Anyone with the link" within the Google Workspace domain. Admins can override the default Setting (Change the link sharing settings) to "Private." Administrators can also create DLP policies that inspect emails for evidence of certain PII/PHI identifiers and apply policy on how that data is shared.



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

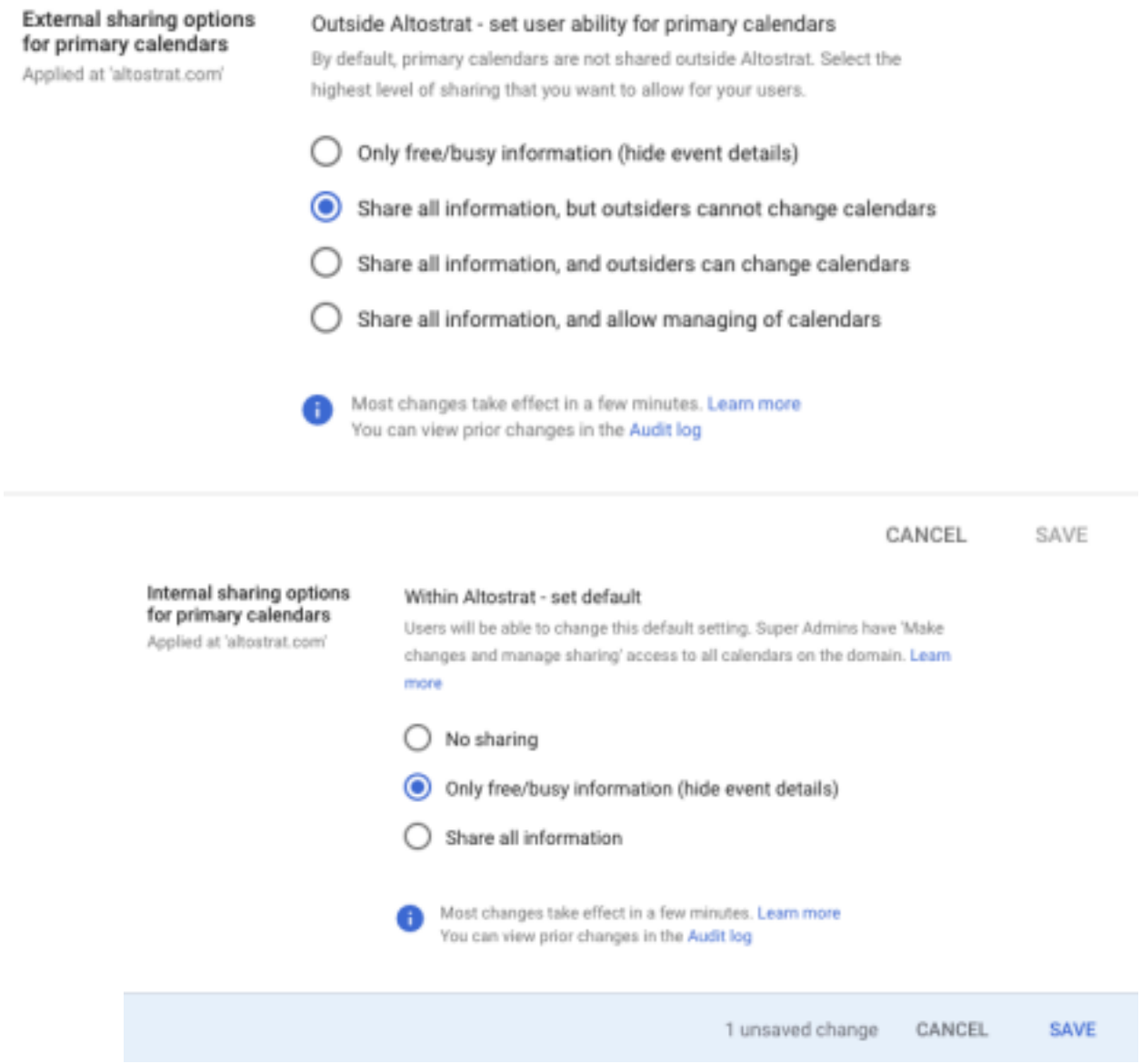
If Gmail is used to email groups of individuals or mailing lists, users are advised to use the "Bcc:" field instead of the "To:" field so recipients of the email are hidden from each other. Additionally, recipients in the "Bcc" field are not copied in subsequent "Reply" and "Reply All" threads.

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. Admins can override the default values and sharing options. If Admins choose to not do so, the responsibility would fall on users to take individual actions to prevent PHI exposure. To limit exposure of PHI within the domain, employees should consider setting calendar

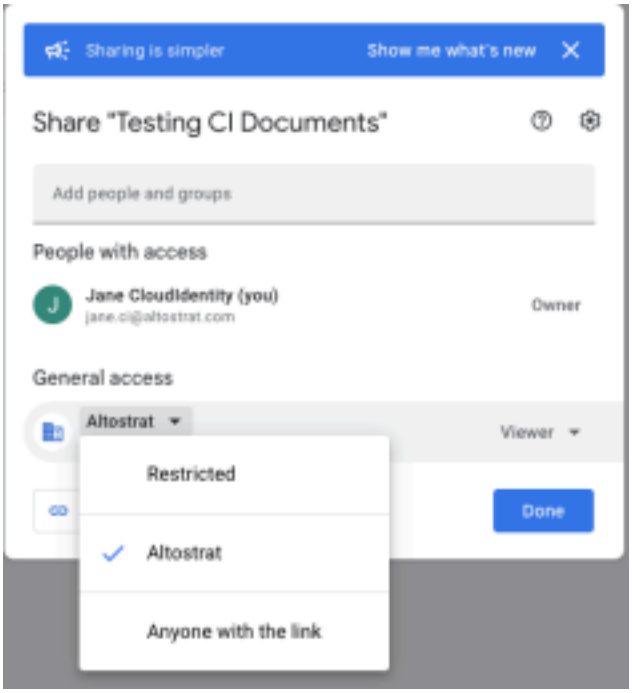
entries to “Private” for calendar entries that contain PHI. Calendar provides a feature that can add a link to a Meet video meeting to the Calendar entry. Please see details below regarding use of Meet for video meetings.

Admins should consider setting external sharing settings to “Only free/busy information" for the domain when PHI is handled. Admins should consider setting internal 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 Shared Drives.



Admins can set file sharing permissions to the appropriate visibility level for the Google Workspace account. Admins can “Restrict” or “Allow” employees to share documents outside the domain, and set the default file visibility to “Private to the owner.”



In addition, admins can also restrict sharing for content within individual Shared Drives or even set defaults for all newly created Shared Drives in an organization. These restrictions can help limit whether Shared Drives may have external users as members, or whether or not members can download, copy and print any of the files in the Shared Drive. For more on Shared Drives, see this article. To learn more about managing sharing within Shared Drives, see this article.

The file exposure reports within the Security Center for Google Workspace give admins information on how employees are sharing files. For example, the report can show which files are shared with external domain users. Admins should consider periodically running these reports for employees who manage PHI to ensure PHI is not inadvertently shared.

Admins should consider disabling third party applications that can be installed, such as apps using the Google Drive SDK API 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.



Data Studio

Data Studio is designed to simplify reporting and dashboarding for Google Workspace users. One of the key features of Data Studio is dashboard sharing.

When a user connects a Data Studio dashboard with an underlying dataset, such as Google Sheets or BigQuery, the user has the option to authenticate using one of three mechanisms:

Authenticate as owner: Always use owner's credentials, regardless of viewer's permissions.	
Authenticate as viewer: Check viewer's credentials against source dataset.	

Authenticate as service account: Always use service account's credentials, regardless of viewer's permissions.



In the example, a user has been granted viewer permissions to a dashboard, but does not have direct permissions to the underlying data source. When a dashboard is configured to authenticate as owner or service account, dashboard viewers can view data regardless of their own permissions. It is recommended that, if using Data Studio, dashboard owners always set "*authenticate as viewer"* when configuring data sources.

While Admin sharing settings can limit Data Studio access to domain users, the features in Data Studio designed to simplify can inadvertently expose data that isn't intended to be shared. It is recommended that users establish strong access governance controls for Data Studio dashboards on PHI to mitigate the risk of inadvertently sharing data.

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. Admins can use audit logs for tracking Apps Script created by Employees in the domain.

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.

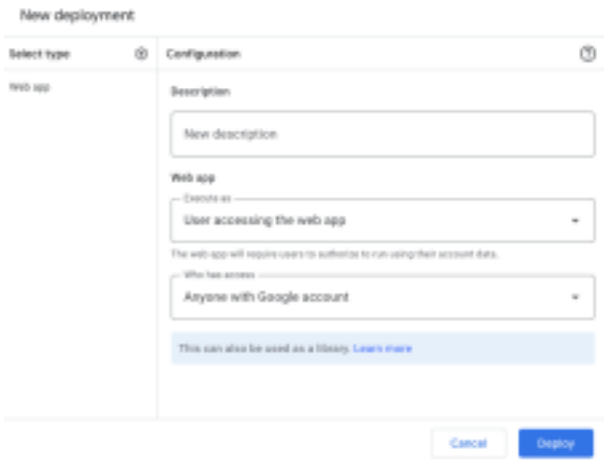
When using the JDBC or UrlFetchApp service, do not insert PHI into an external database or upload it to an external web service unless the database or web service is only accessible to users who are authorized to access PHI. Do not use JDBC or UrlFetchApp to insert or upload PHI to Google Cloud Platform 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 it 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.

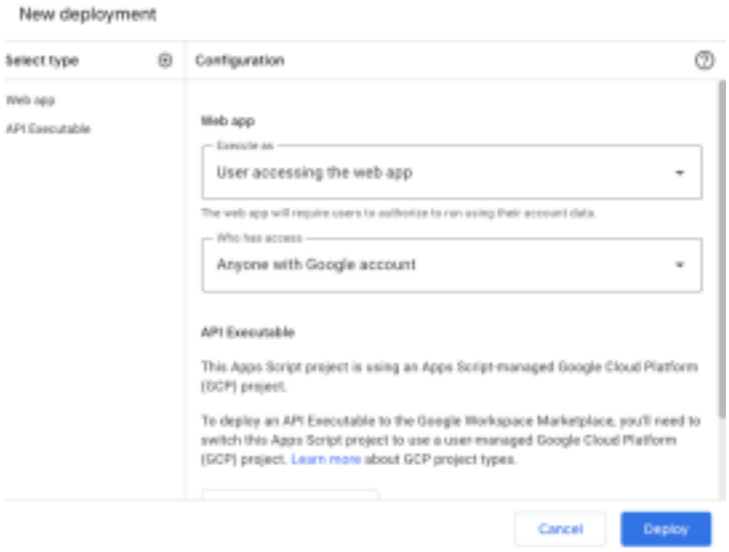
When deploying an Apps Script project that handles PHI as a web app, under "Execute the app as," it is recommended to select "User accessing the web app."

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

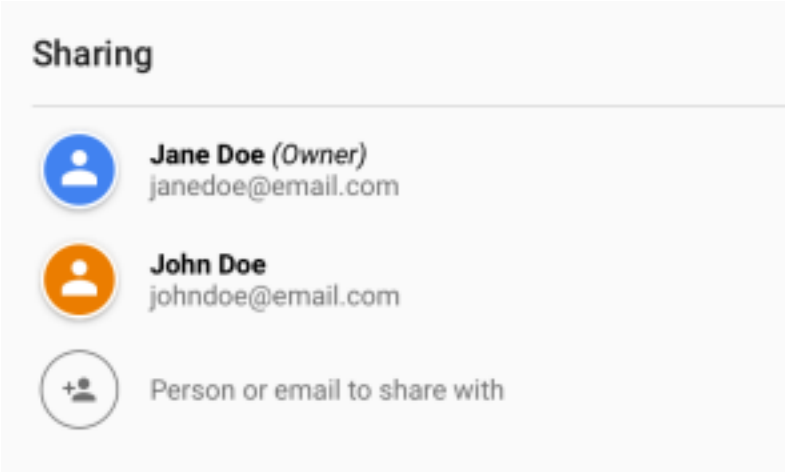
Within your domain, employees can use Keep to take notes and create lists containing PHI. In Drive sharing settings, Admins can set file sharing permissions to the appropriate visibility level for the Google Workspace account. Admins can “Restrict” or “Allow” employees to share documents outside the domain, and set the default file visibility to “Private.”



Key note: the sharing settings for notes created in Google Keep are a subset 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 Delete the note, which will delete the note for all collaborators as well. Collaborators on a note are not able to delete the note, however, they can choose to unsubscribe from the note if they choose.

Sites

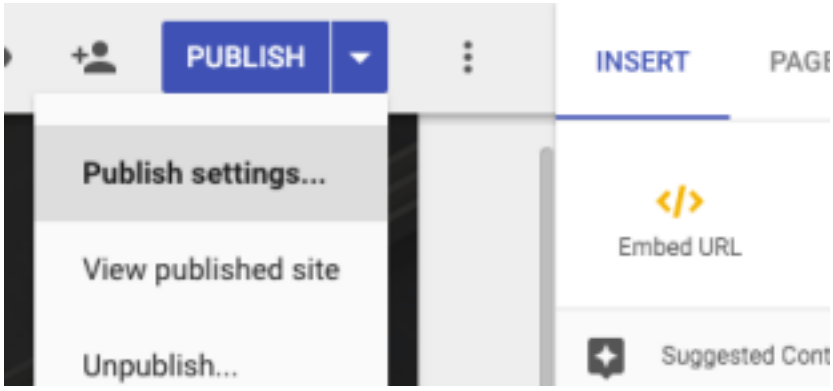
The Google Sites service, like all Google Workspace Core Services, does not serve advertising or use customer data for advertising purposes. However, some users of AdSense may use the separate AdSense product to display advertising on their Sites pages. Users should ensure that AdSense is not included whenever Google Sites is used with PHI.

For Google Sites containing PHI, employees should configure the Sites sharing and visibility settings appropriately. PHI can be included in a site in the form of text, images, or other content (such as a Google Calendar or content stored in Google Drive (including Docs, Sheets, Slides, and Forms). Instructions to configure these settings are outlined below:

Sites

The most recent 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. Admins may also create an internal approval process within their organization to ensure there is no unintended disclosure of PHI in the sites before being published by Employees.



Sharing settings

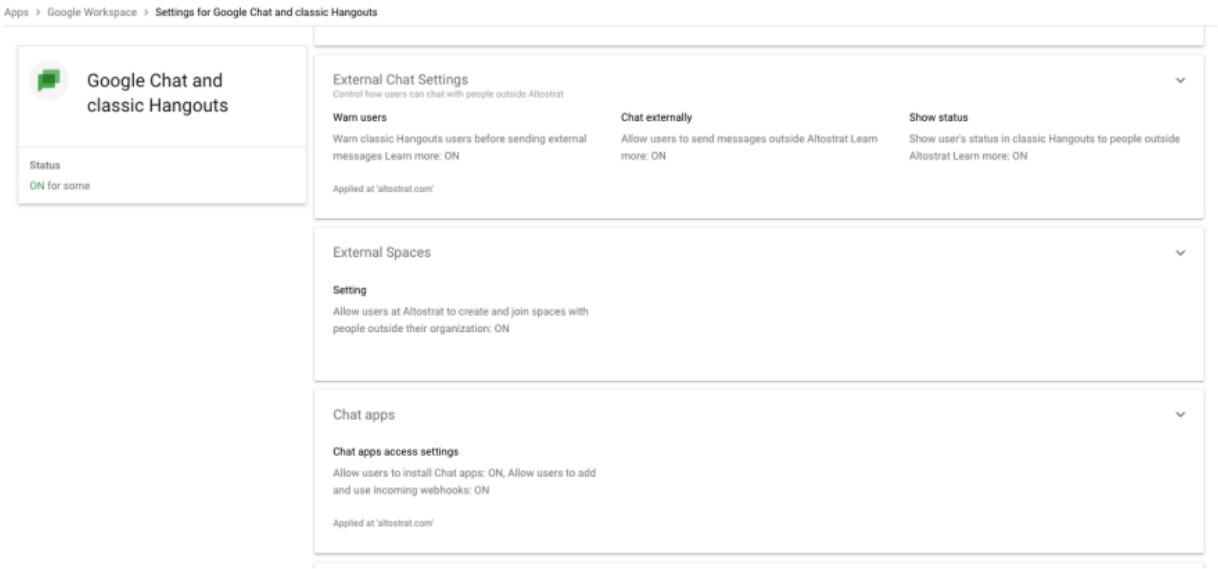
In Drive sharing settings, Admins can set file sharing permissions to the appropriate visibility level for the Google Workspace account. Admins can “Restrict” or “Allow” employees to share documents outside the domain, and set the default file visibility to “Private.”

Google Chat

Chat provides several options for Admins to control sharing PHI. Chat can be enabled or disabled for everyone in the domain or selectively enabled for specific organizations.

To enable the service for specific organizations, Admins can select the ‘ON for some organizations’ option which displays the Org Units to search and select.

Note that Chat now supports cross domain and external communication, refer to this article and blog post for details.



It is recommended that users create a new Chat Space when adding multiple members to a chat conversation. Additionally, users should refrain from using PHI in room naming. New members that are added to Chat Spaces will be able to see previous chat history. Invitees can preview the Chat Space and read messages. Users are recommended to delete chat messages containing PHI.

Sharing options

Users 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 Shared Drives.

Admins can set file sharing permissions to the appropriate visibility level for the Google Workspace account. Admins can “Restrict” or “Allow” employees to share documents outside the domain, and set the default file visibility to “Private.”

When sharing Google Drive files (including Docs, Sheets, Slides, and Forms) to a Chat Space, all members of the Space are granted “Comment Access” to the file. This will not overwrite sharing permissions set up by an Admin. New members of the Space will be granted “Comment Access” to all files that have previously been shared in the room.

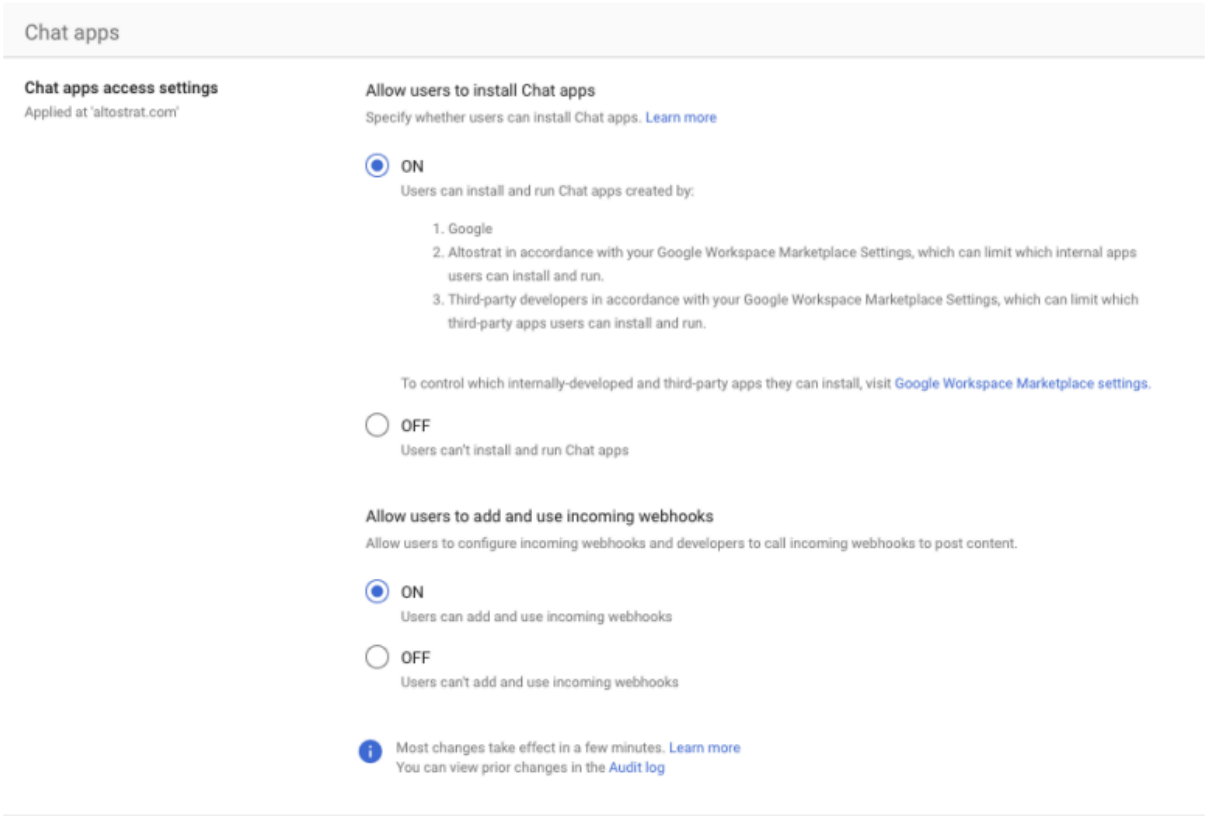
If a member has been removed from the Space, they will lose “Comment Access” to all files that have been shared in the room unless they continue to have access through other means such as membership of other Spaces where the document is shared, or shared directly with the member.

Admins can set up DLP rules to prevent data leakage in Chat. Here are some instructions on how to configure DLP for Chat.

Bots and integrations

Bots and integrations are controlled using the “Chat Apps” settings. Google offers two Chat apps that integrate with other Google Workspace services: @meet and @drive. Third party developers can also create Chat Apps as a bot for use with Chat. Admins should carefully consider disabling Apps and integrations, by unchecking the following item under Chat Settings:

❏ Allow users to install Chat apps



@Meet by Google

@Meet is a meeting scheduling bot that can be used within Chat. This bot has been designed to follow the Calendar sharing settings set by the domain and end user. Please refer to "Use the @Meet bot" for additional guidelines on the usage of @Meet.

@Drive by Google

@Drive is a file management bot that can be used within Chat. It will notify users when new

files are shared with them, when new comments are made on files, or when someone else requests access This bot has been designed to interoperate with Drive sharing settings set by the domain and end user. "Use the Google Drive App" for additional guidelines on the usage of @Drive.

Third party apps and integrations

Admins should review the security of these applications, as well as any corresponding security and privacy documentation provided by the third party developer.

Google Meet (Google's video meeting experience)

Google Meet, the video meeting experience by Google, supports HIPAA compliance.

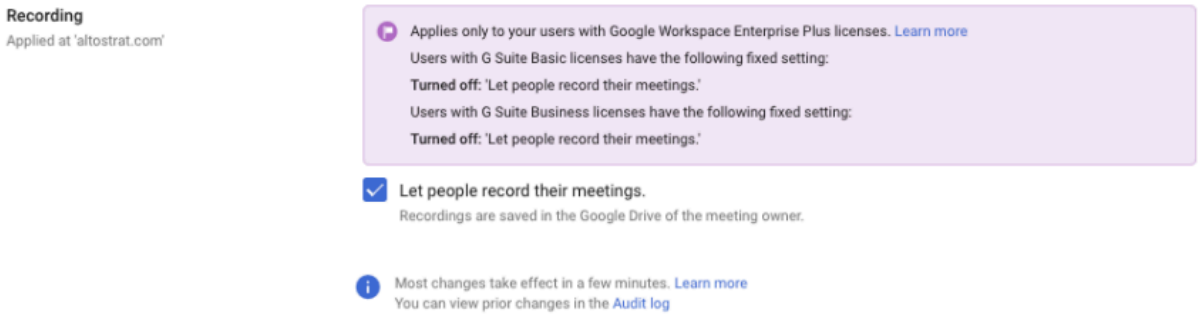
Meet allows you to control whether external guests may participate in each video meeting. People in the same Google Workspace domain can manage external guest access by controlling who gets invited to the meeting, determining whether to permit anonymous guests to join a running video call, and removing unwanted participants from the call. Please see the Meet support pages for more information on inviting guests, and the “Meet dialing to GV users” section below for more details on the information that is displayed when dialing out to a Google Voice user.

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, unless the call is recorded.

Meet allows Google Workspace Enterprise 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 in Google Drive. Similarly if Meet Transcription was enabled during the call, the transcribed text of the meeting is also saved in Google Drive and follows Drive sharing permissions. Google Meet allows users to present their screen during the meeting. Host of the meeting can allow or restrict other attendees from sharing their screen. Users who are presenting their screen are accountable when sharing appropriate PHI / PII data on their screen during the meeting.

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



Meet Dialing to GV Users

Google Voice users will see Meet meeting names displayed on their devices when a Meet meeting participant dials out to the Google Voice user from within a Meet meeting. The meeting name will only be displayed if the Google Voice user is on the meeting invite, is in the same domain as the meeting creator and the calendar invite is visible to users in the domain, or if the meeting creator's calendar is publicly shared.

To limit exposure to PHI when a Google Voice user is dialed into a Meet meeting, users should consider setting calendar entries to "Private" for calendar entries that contain PHI. Admins should consider setting external Calendar settings to "Only free/busy information" and internal Calendar sharing options to "No sharing" or "Only free/busy information."

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.

When using connectors to share third party data with Google Cloud Search Platform edition, customers are responsible for ensuring access controls and permission settings are accurately configured based on the organization's data use policies.

When building connectors to index their third party data, customers should apply the individual document access and permission settings through the connector so it can be interpreted accordingly by Cloud Search when indexing and servicing content to users. PHI in document titles and descriptions may be exposed to individuals as search results if a connector application does not properly translate the access and permission settings in a third party data store. More guidance on Cloud Search Connectors and access and permission settings is available here.

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

Cloud Identity Management

Cloud Identity Management is an Identity-as-a-Service (IDaaS) solution that provides a centralized console to manage users, apps and devices. If you need to store PHI information, custom user attributes is the only place you can store user's PHI information.

When you create a user account, Cloud Identity Management provides predefined user profile attributes such as employee ID, location and title.You can create custom attributes, if you would like to store any other information about the user that is not part of predefined attributes. With custom attributes, you can:

- Add more user data you want to record; for example, assign different data types to special value fields, such as number, date, and email.
- Control whether you want the information to be public to all users in your organization, or private to administrators and the individual user.

For additional information on how to create and manage custom attributes, please review this help center article.

If you decide to store PHI information in the custom attributes, we strongly recommend you to make the custom attribute as "Private". This will make the custom attribute visible only to the individual user and the delegated or super administrators who have 'read' or 'edit' privileges to the user profiles. If you do not set the 'Private' flag, then the custom attribute will be accessible to all users in the domain. Detailed instructions are available in the "add a new custom attribute" section in this help center article. In addition to using the admin console, you can use the following ways to create custom attributes.

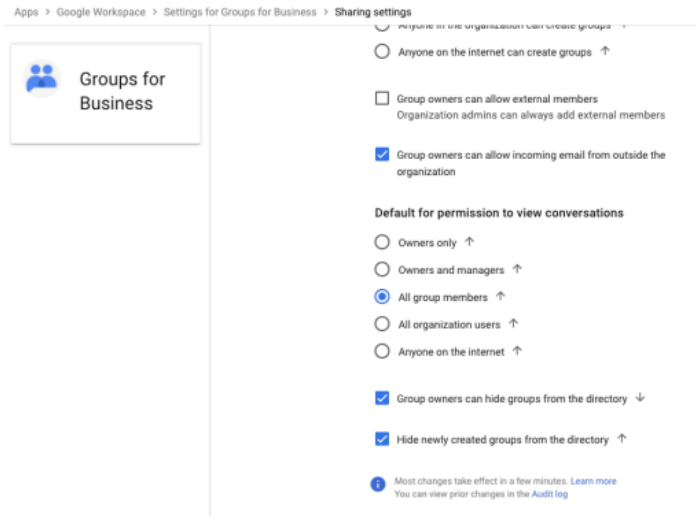
- Admin SDK: please review this help center article for additional information on creating, managing, or setting up security for customer attributes. Pay close attention to read AccessType while creating a custom Schema and please note the 'Private' flag is known as "ADMINS_AND_SELF" in the API.
- Google Cloud Directory sync (GCDS): please review this help center article for additional information on creating, managing, or setting up security for custom attributes. Pay close attention to **Read Access Type** setting. This setting controls the read access to the field data defined in the schema fields.

Groups

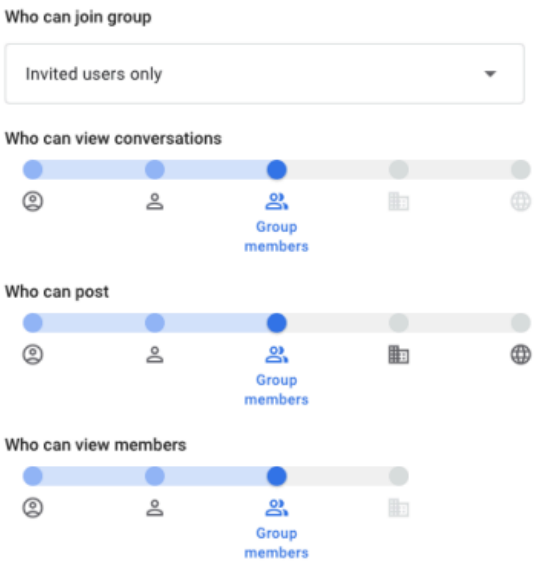
Admins should review the sharing options in the Groups admin console settings in order to appropriately restrict outside domain access, default discoverability, and default view

topics permission of newly created groups.

For groups containing PHI, admins should consider setting access to groups to “Private”, which will restrict all Groups created on the domain from visibility outside the domain. Admins or group owners may also set the default “View topics” permission to at most “All members of the group” to restrict access to the web posts and email archive of the group.



Individual group owners can access additional permissions located under the “Manage > Permissions” section of the group’s settings. These elections further control access to who can join and view, post, edit, and delete posts within a specific group.



Groups posts are stored until deleted by a user. The email archive of a group can be deleted via “Manage > Information > Advanced” section. Note that deleting a group is permanent and deletes everything related to the group including memberships.

If creating groups to manage mailing lists, careful consideration should be made when naming and emailing the group so it does not expose the PHI of the members of the group. Using the “to:” field instead of the “bcc:” field when emailing groups (i.e. mailing lists) will expose any individual that “Reply all” to the email as other recipients on the email thread will be able to see the individual's response.

If Groups is used as a collaborative inbox, note that all collaborators will be able to see emails sent to the collaborative inbox and access should be restricted accordingly. Any PHI that is sent to or from the collaborative inbox will be visible to all collaborators and may expose an individual's PHI. Careful consideration should be made when naming the collaborative inbox so PHI would not be exposed when individuals receive emails from such inboxes.

Google Voice (managed users only)

Licensed users of Google Voice are covered under the Google Workspace BAA. Administrators should obtain Google Voice licenses for users that handle PHI. Please refer to Assign Google Voice licenses and Migrate existing users to managed accounts.

For additional HIPAA considerations on dialing Google Voice users via Meet, see the Meet dialing to GV users section.

Tasks

Administrators may turn the Tasks service on/off in the Admin console. Information stored in Tasks is always private for the individual and should not be visible to other users or outside the organization.

Gemini in Workspace

When using Gemini in Workspace with PHI within the applicable HIPAA Included Functionality, the same recommendations provided in this guide will apply. Enterprise end users can submit feedback regarding their experience using generative AI features. End users are informed before submitting the feedback that feedback data should not contain personal, sensitive, or confidential information.

Gemini app as a Google Workspace Core Service (excluding Gemini in Chrome)

When using the Gemini app as a Google Workspace Core Service via gemini.google.com or

mobile application with PHI within the applicable HIPAA Included Functionality, the same recommendations provided in this guide will apply. Access to the Gemini app via Gemini in Chrome is not HIPAA compliant and customers should not upload PHI into Gemini in Chrome. Administrators who do not wish to offer access to the Gemini app via Gemini in Chrome should turn off access to Gemini in Chrome. Click here to learn more about how to manage user access to Gemini in Chrome.

Access to Gemini app as an Additional Product is not HIPAA compliant and customers should not upload PHI into the Gemini app in this scenario. Administrators who do not wish to offer access to the Gemini app as an Additional Product should only turn on access to the Gemini app as a Workspace Core Service. Click here to learn more about how to manage user access to the Gemini app.

Workspace Studio

When using Workspace Studio with PHI within the applicable HIPAA Included Functionality, the same recommendations provided in this guide will apply. Workspace Studio allows users to build workflows and AI steps that read from and write to other Google Workspace Core Services such as Gmail, Google Drive, and Google Chat. The sharing and access recommendations in those sections apply to any data a workflow processes; it is recommended that workflows handling PHI are created and shared only with users who are permitted to access that PHI.

Administrators can turn Workspace Studio on or off in the Admin console (Apps > Google Workspace > Workspace Studio > Service status), including for specific organizational units or access groups, and should consider limiting access to users who require it. Turning the service off for a user stops any active flows they own. Click here to learn more about how to manage user access to Workspace Studio. Workflows that connect to third-party applications or services are subject to the guidance in the "Use of third party applications, systems, or databases" section; such connections are not covered by the BAA.

When using AI steps within Workspace Studio with PHI, the same recommendations provided in the "Gemini in Workspace" section apply.

Additional considerations for HIPAA compliance

Separating user access within your domain

To manage end user access to different sets of Google services, a Google Workspace 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 Google Workspace account, for instance, there are typically two or three organizational units. The largest unit includes employees with most services enabled, including YouTube; another unit is for employees who may manage PHI, with certain services disabled. In a more complex Google Workspace 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, systems, or databases

If an end user wants to use the HIPAA Included Functionality to share PHI with a third party (or a third party application, add-on, system, or database), including through authorizing API access to PHI, 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, add-on, system or database) 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 Google Workspace 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 all organizations with Enterprise or Cloud Identity licenses review the security health tool, which provides recommendations on how to improve your security posture. All organizations can see these security recommendations in the Help Center articles here and here.

Security audits and certifications

A list of security and privacy controls available with Google Workspace can be found on our Google Workspace Admin help center.

In addition to supporting HIPAA compliance, the Google Workspace Core Services are audited

using industry standards such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and SOC 1/2/3 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 and compliance controls, we've made our ISO/IEC certificates and SOC audit reports available for download via Compliance Reports Manager.

Additional resources

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

- Google Workspace Help Center
- Google Workspace security page
- HIPAA Compliance with Google Workspace
- Google Cloud HIPAA compliance page
- Google Cloud Healthcare and life sciences compliance page
- Google Cloud Compliance Resource Center

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.