

HIPAA Compliance & Data Protection with G Suite

G Suite HIPAA Implementation Guide

Table of Contents

Customer Responsibilities	3
Using Google Services with PHI	3
What to Consider for Specific G Suite Core Services	5
Monitoring account activity	5
Gmail	6
Calendar	6
Drive (including Docs, Sheets, Slides, and Forms)	7
Cloud Search	9
Sites	9
Additional Considerations for HIPAA Compliance	11
Separating user access within your domain	11
Use of third party applications	12
Security best practices	13
Security Audits and Certifications	13
Additional Resources	13

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), [Google Apps 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, Google Calendar, Google Drive (including Docs, Sheets, Slides, and Forms), Google Cloud Search, Google Sites, and Google 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 Services¹, which may include Hangouts, 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
Google Calendar
Google Drive (including Docs, Sheets, Slides, and Forms)
Google Cloud Search
Google Sites
Google Vault (if applicable)

Core Services in which PHI is <u>not</u> permitted
Google Hangouts
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

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

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

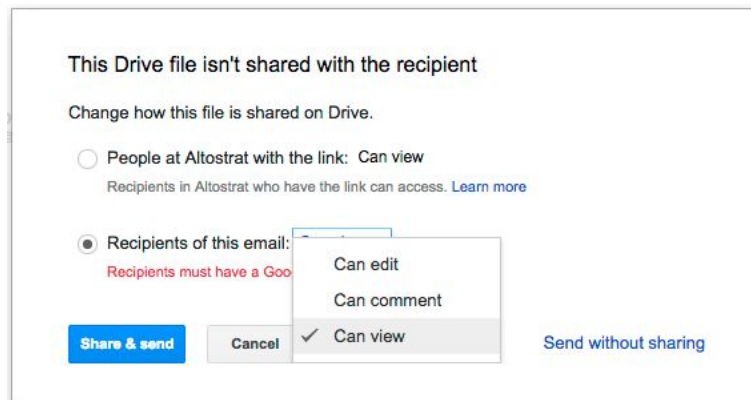
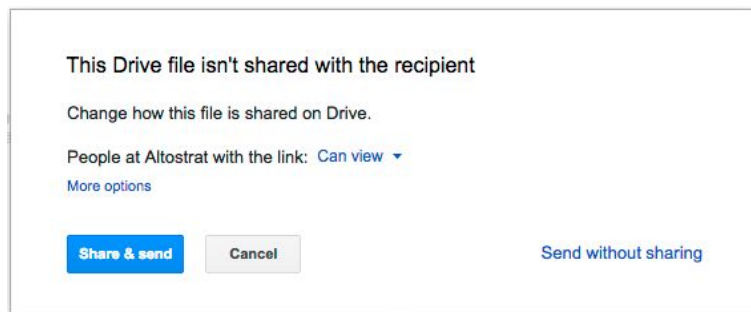
Every G Suite Core Service has specific settings to adjust to help ensure that data is secure, used, and accessed only in accordance with your requirements. Here are some actionable recommendations to help you address specific concerns within services that are HIPAA Included Functionality:

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.

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.”



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. Hangouts is not part of the [Included Functionality](#) and should not be used with PHI.

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

Video Calls
Locally applied

Automatically add video calls to events created by a user

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

External sharing options for primary calendars
Locally applied

Outside Altostrat - set user ability for primary calendars

By default, primary calendars are not shared outside Altostrat . Select the highest level of sharing that you want to allow for your users.

- Only free/busy information (hide event details)
- Share all information, but outsiders cannot change calendars
- Share all information, and outsiders can change calendars
- Share all information, and allow managing of calendars

Internal sharing options for primary calendars
Locally applied

Within Altostrat - set default

Users will be able to change this default setting. Super Admins have 'Make changes and manage sharing' access to all calendars on the domain.






[Learn more](#)

- No sharing
- Only free/busy information (hide event details)
- Share all information

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.

Link sharing

-  **On - Public on the web**
Anyone on the Internet can find and access. No sign-in required.
-  **On - Anyone with the link**
Anyone who has the link can access. No sign-in required.
-  **On - Altostrat**
People at Altostrat can find and access.
-  **On - People at Altostrat with the link**
People at Altostrat who have the link can access.
-  **Off - Specific people**
Shared with specific people.

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.”

Link Sharing

Locally applied

Link Sharing Defaults

Select the default link sharing setting for a newly created file:

- OFF**
Only the owner has access until he or she shares the file.
- ON - People at admin.altostrat.com with the link**
People at admin.altostrat.com who have the link can access the file.
- ON - People at admin.altostrat.com**
People at admin.altostrat.com can find and access the file.

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.

- Allow users to install Google Drive apps**
Google Drive apps allow users to open their files in web apps installed from the Chrome Web Store. [?](#)
- Allow users to install Google Docs add-ons**
Docs add-ons allow users to use Docs features built by other developers. [?](#)

Cloud Search

Admins can control the use of search history with 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 this [article](#).

Sites

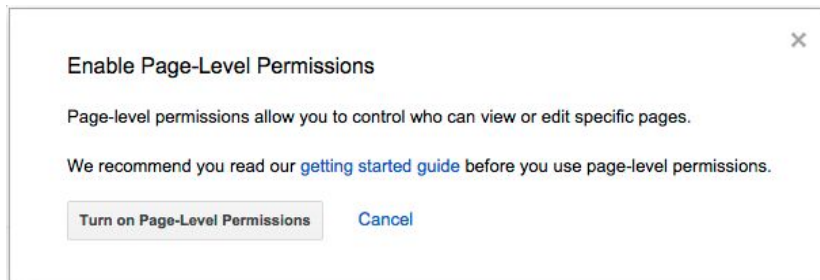
The Sites service (both classic and new versions), like all G Suite Core Services, does not serve advertising or use customer data for advertising purposes, however, some legacy users of AdSense on the classic version of Sites may [retain the ability to use the separate AdSense product](#) to display 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."](#)

Site Visibility
Locally applied

Visibility of Sites
Select the default visibility for newly created sites:

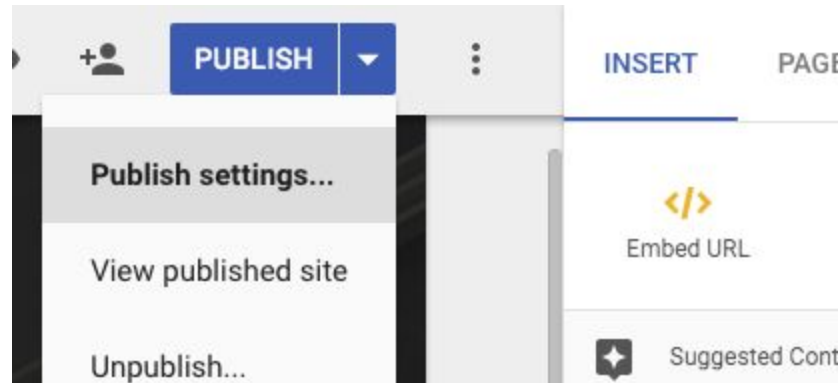
- Users at Altostrat can find and edit sites
- Private (only visible to site owner)



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.

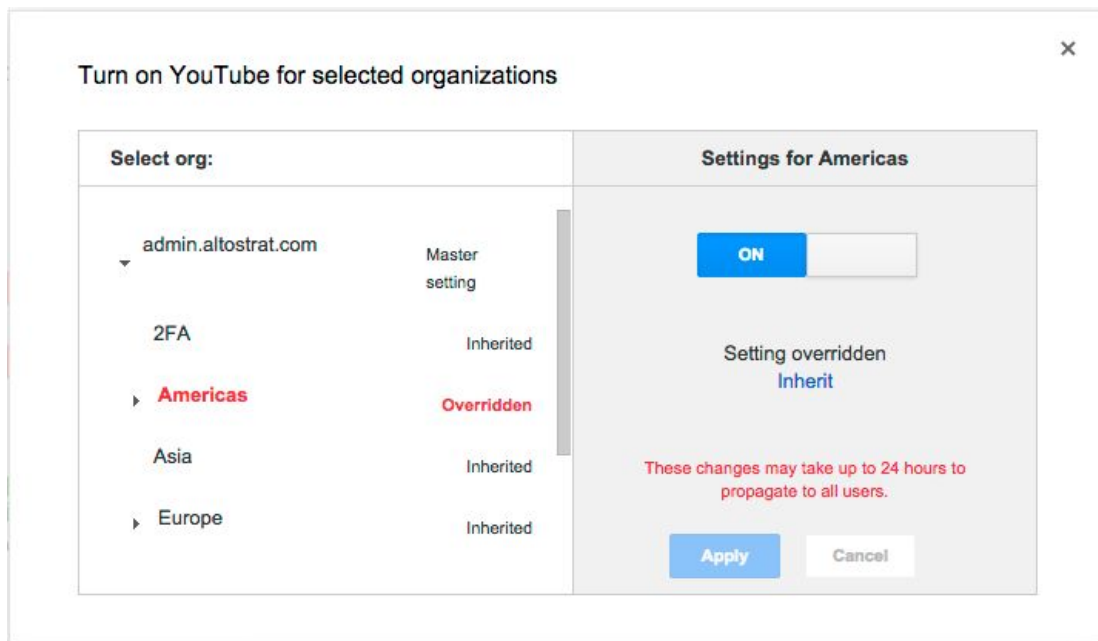
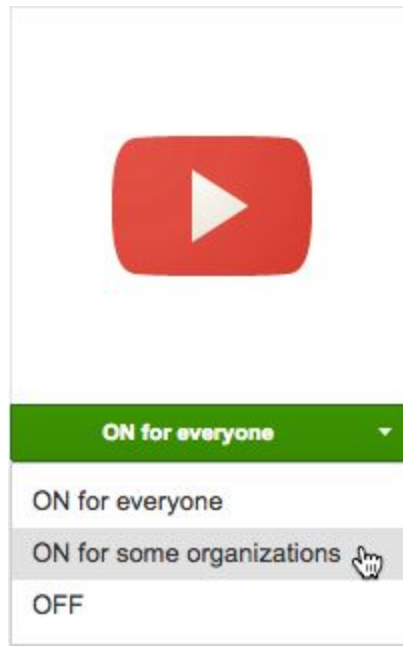
Additional Considerations for HIPAA Compliance

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.

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.