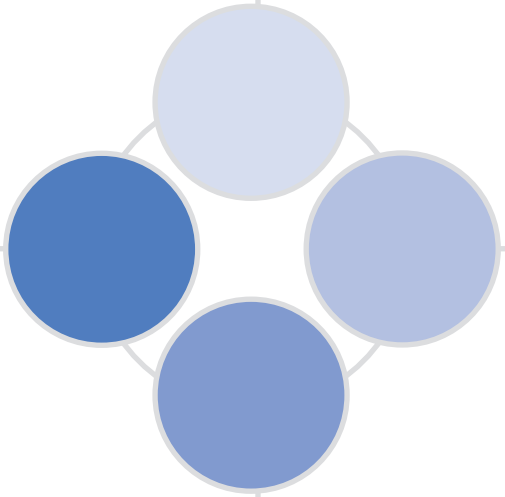
HIPAA Compliance & Data Protection with Google Apps

Google Apps for Work HIPAA implementation guide

Google™ for Work

HIPAA Compliance & Data Protection with Google Apps



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 Google Apps. 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. 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.

Using Google Services with PHI

Google Apps customers who are subject to HIPAA and wish to use Google Apps with PHI must sign a Business Associate Agreement (BAA) with Google. Per the Google 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 Apps Core Services ("Core Services") covered by your Google Apps Agreement into three categories. Google Apps 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 Google Apps HIPAA BAA as long as the health care organization configures those services to be HIPAA compliant:** Gmail, Google Drive (including Docs, Sheets, Slides, and Forms), Google Calendar, Google Sites, and Google Apps Vault (see full list of Google Apps Core Services here).

2. **Core Services where PHI is *not* permitted: There are certain remaining Core Services that may not be used in connection with PHI.** Google Apps administrators can choose to turn on these remaining Core Services, which include Hangouts, Contacts, and Groups, for its users, but it is their responsibility to not store or manage PHI in those services. Please see "Separating user access within your domain" for further details on how to utilize organizational units.

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 Apps Agreement, including, for example, (without limitation) YouTube, Google+, Blogger, and Picasa Web Albums (see list of Additional Google Services here), must be disabled for Google Apps users who manage PHI within the Included Functionality. 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 manage end user access to different sets of Google services, Google Apps 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 YouTube and Google+ 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 Google Apps security whitepaper.

What to Consider for Specific Google Apps Core Services

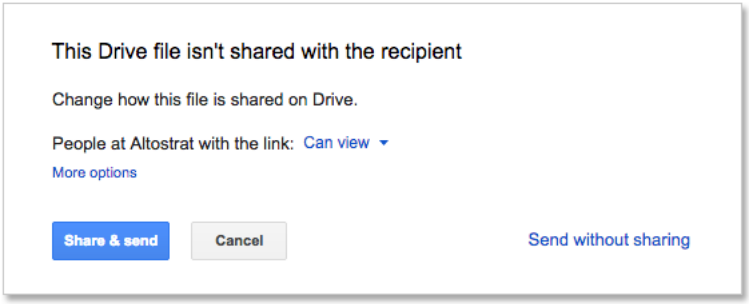
Every Google Apps Core Service has specific settings to adjust to help ensure that data is secure, used, and accessed only in accordance with your requirements. Here are some actionable recommendations:

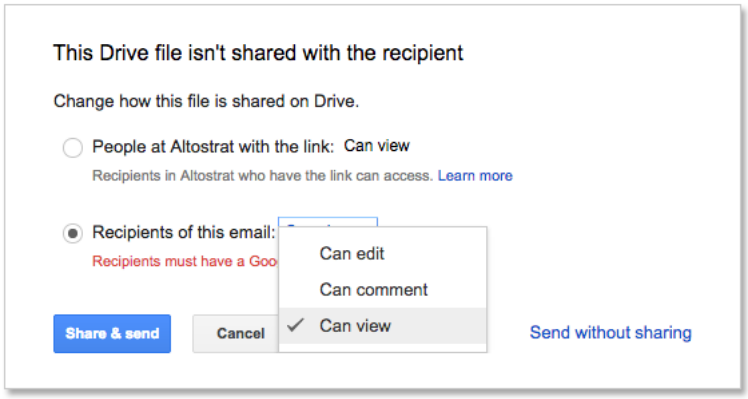
Monitoring account activity

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

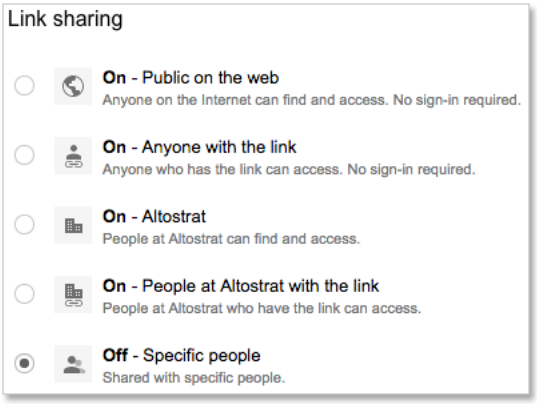
Gmail provides controls to ensure that messages and attachments are only shared with the intended recipients. When composing emails and inserting files using Google Drive that potentially contain PHI, end users can choose to share only with the intended recipients. If the file is not already shared with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



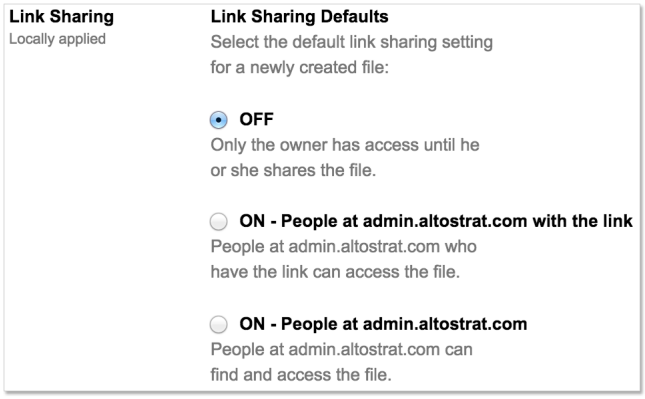


Drive (including Docs, Sheets, Slides, and Forms)

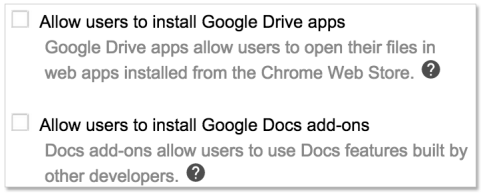
Employees can choose how visible files and folders are, as well as the editing and sharing capabilities of collaborators, when sharing files in Google Drive (including Docs, Sheets, Slides, and Forms).



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

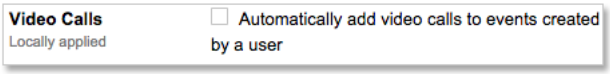


Admins should consider disabling third party applications that can be installed, such as Google Drive apps and Google Docs add-ons. Admins should review the security of these applications, as well as any corresponding security documentation provided by the third party developer.

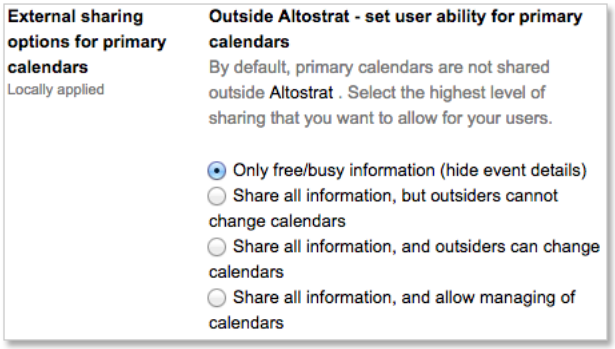


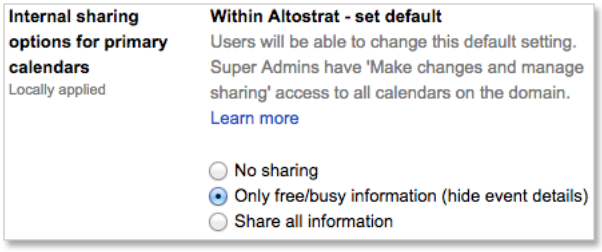
Calendar

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. Employees should consider setting calendar entries to "Private" for meetings involving PHI. In addition, employees should consider excluding PHI from meeting titles, descriptions, and Hangout video calls, unless proper privacy settings have been applied. Admins should consider disabling the option to automatically add Hangout video calls for employees who manage PHI.



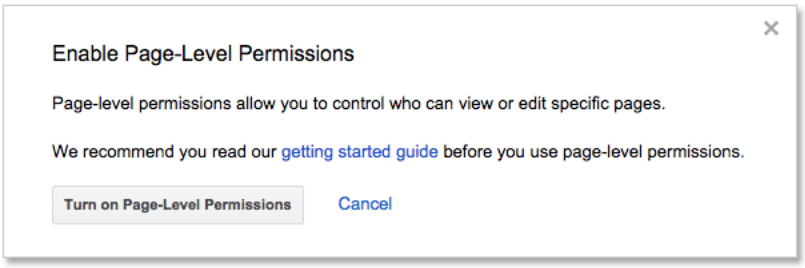
Admins should consider setting calendar sharing options to "No sharing" or "Only free/busy information" for employees who handle PHI.



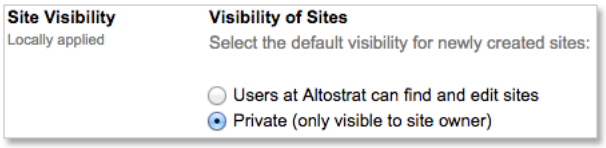


Sites

For Sites containing PHI, employees should consider setting the share settings to "Private." Employees can also turn on page-level permissions to granularly control who has access to individual web pages within a Site.



Employees should consider setting 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."



The Google Sites service, like all Google Apps Core Services, does not serve advertising or use Customer Data for advertising purposes. However, some legacy users of AdSense on Sites may retain the ability to use the separate AdSense product to display advertising on their Sites pages. Users should ensure that AdSense on Sites is disabled whenever Sites is used with PHI.

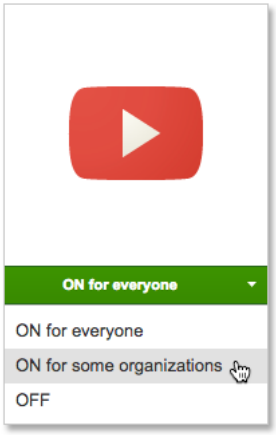
Additional Considerations for HIPAA Compliance

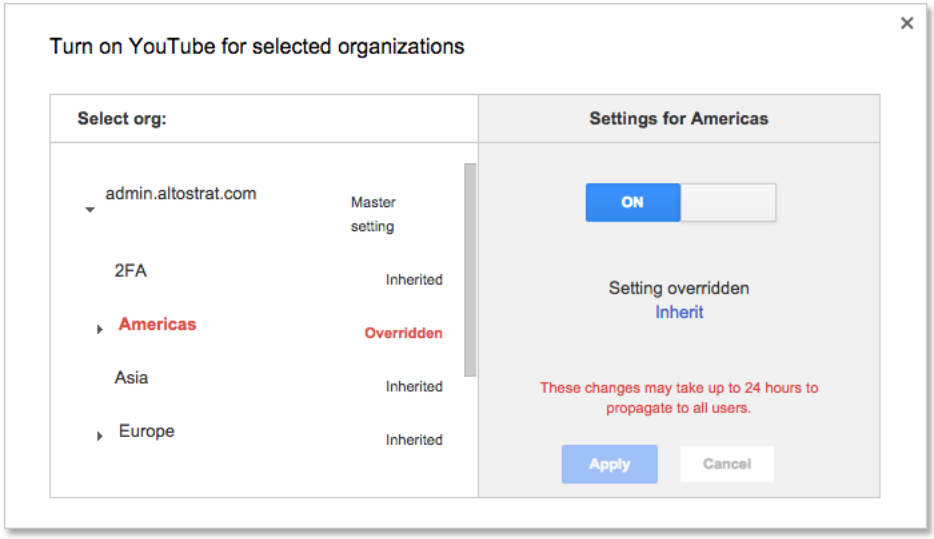
Separating user access within your domain

To manage end user access to different sets of Google services, a Google Apps 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 Apps 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 Google Apps 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 Google Apps 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 Google Apps can be found on our Security and Privacy website.

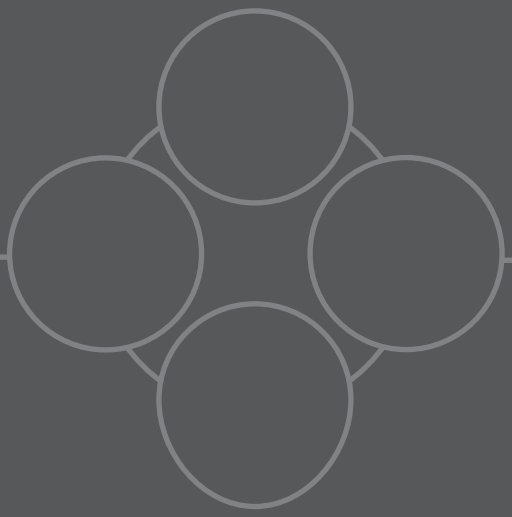
In addition to supporting HIPAA compliance, the Google Apps Core Services are audited using industry standards such as ISO 27001 certification and SOC 2 and SOC 3 Type II audits, which are the most widely recognized, internationally accepted independent security compliance audits. To make it easier for everyone to verify our security, we've published our ISO 27001 certificate and new 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.

- Google Apps Help Center
- Google for Work security page
- HIPAA Compliance with Google Apps

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.



Google™ for Work