

Is Gmail HIPAA Compliant?



Inside this guide:

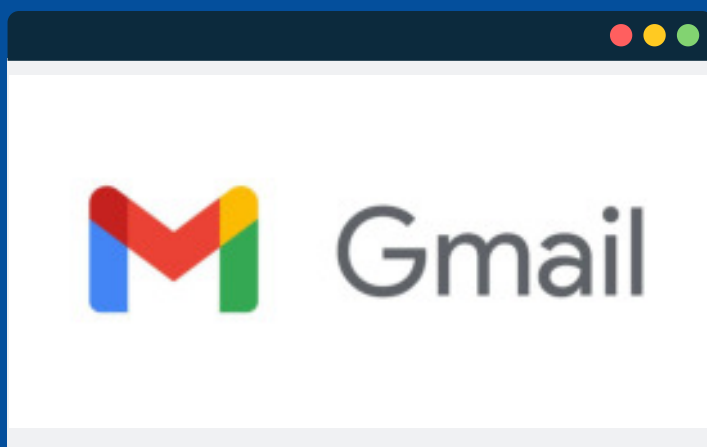
HIPAA Basics

How to make Gmail HIPAA compliant



Is Gmail HIPAA Compliant?

Google applications have long been a standard resource for businesses. But when it comes to health care practices, how do you know if your sensitive patient data is being kept safe?



HIPAA Basics

Google has safeguards in place that can successfully keep protected health information (PHI) secure during email transmission. HIPAA regulation demands that safeguards be put in place to keep PHI secure when it is transmitted electronically (also known as electronic protected health information, or ePHI).

These safeguards are outlined in the HIPAA Security Rule, which was first published in 2003, and went into effect in 2005. Since then, all transmissions of ePHI by HIPAA-beholden entities have been subject to federal regulatory standards.

Before we start, here are a few key HIPAA definitions you should be familiar with in order to understand your regulatory obligations.

HIPAA Definitions

- **Covered Entity (CE):** A health plan or a health care provider who stores or transmits any health information in electronic form in connection with a HIPAA transaction.
- **Business Associate (BA):** Any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization who, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI. Examples include: storage services, MSPs, IT providers, lawyers, billing services, shredding services, and cloud storage providers, to name a few.
- **Business Associate Agreement (BAA):** A contract entered into between two HIPAA-beholden entities (either between a CE and BA or between two BAs). A good BAA defines liability in the event of a PHI breach. It acknowledges that both entities entering into the agreement will handle PHI in accordance with HIPAA regulation. BAAs must be executed before any PHI can be legally shared.
- **Protected Health Information (PHI):** Any information collected by a CE that can be used to identify a patient or their health records is considered PHI. This includes name, address, date of birth, phone number, email address, social security number, medical record number, health insurance ID number, or full facial photograph, among others. Electronic PHI (ePHI) is any PHI maintained in an electronic format, including electronic health records (EHR).

How to Make Gmail HIPAA Compliant

Using Gmail with PHI

Before you begin using Gmail to transmit or handle PHI, you must sign a G Suite Business Associate Agreement (BAA) with Google. By signing this BAA, you will be able to use Google's Included Functionality with PHI.

Please carefully review this BAA and seek attorney counsel if you have any concerns about your liability.

Google Included Functionality

Be advised that only certain Google tools can be made HIPAA compliant. Google clearly outlines the tools in its G Suite Services that can be HIPAA compliant.

These include:

- Gmail
- Google Calendar
- Google Drive (including Docs, Sheets, Slides, and Forms)
- Google Hangouts (chat messaging feature only)
- Hangouts Meet
- Google Keep
- Cloud Search Google Sites
- Google Vault



If a tool included in G Suite is not listed above, you cannot change its settings to be HIPAA compliant. This includes Google Photos, YouTube, and Contacts, among many others. Any data stored or transmitted via a G Suite service not listed in the Included Functionality above will not comply with federal HIPAA regulation and could lead to a breach of sensitive information or potential HIPAA violations.

Making Gmail HIPAA Compliant Within Your Organization

If you use Gmail, you can use certain advanced settings to make your data transmissions HIPAA compliant.

But first, please be aware that these settings are **ONLY AVAILABLE** to users with a paid G Suite business account. If you utilize a free Gmail account, you cannot use it to transmit ePHI in a HIPAA compliant manner, and you should not do so.

You risk a serious breach of data, and potential HIPAA violations if you try to send ePHI via a free Gmail account.

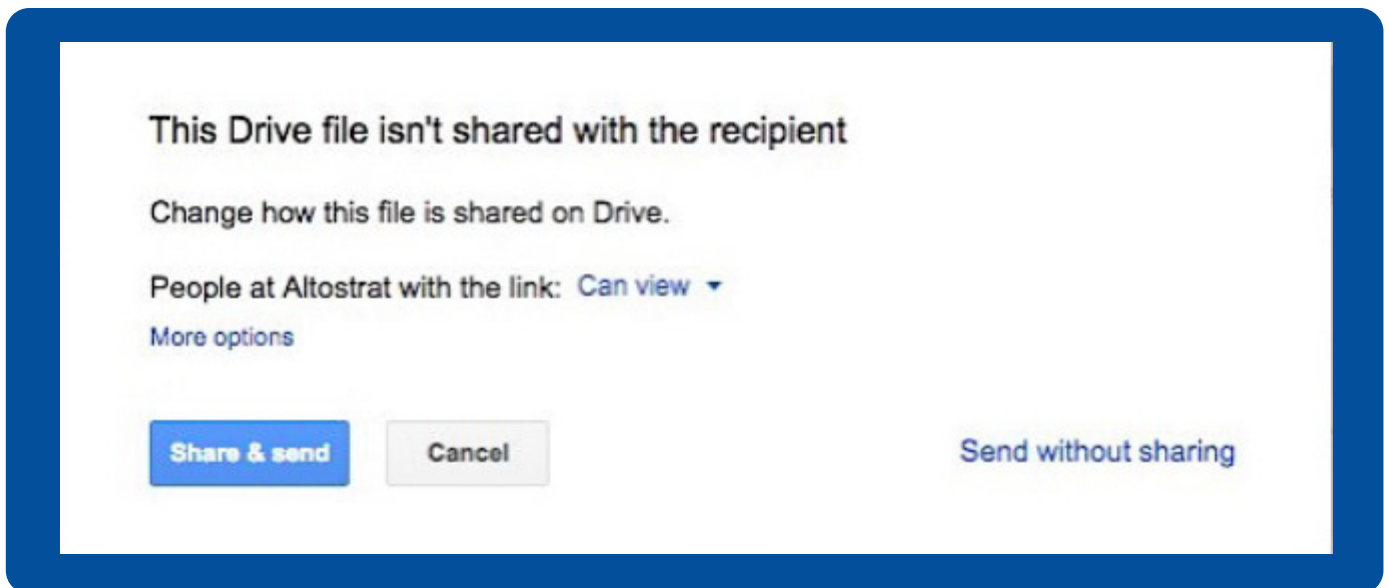
If you have a paid account, Gmail has several settings that you must access in order to make your data transmissions HIPAA compliant.

Gmail has controls to ensure that messages and attachments containing PHI are only shared with the intended parties. Google Drive files that are attached to an email must be individually maintained and monitored to ensure that they are shared with individual end-users or members of your workforce.

A member of your workforce can choose to "share only with intended recipients" when sending emails and attaching files using Google Drive that contain ePHI. This is an access control that allows members of your workforce to monitor who, within your organization, may view each file.

If the file attached to the email has not been shared with all email recipients, Gmail will default to share the file with "Anyone with the link," within the G Suite domain. **Make sure to change the link sharing settings to "Private" in order to keep ePHI secure!**

See the screenshots below for an example of Gmail's access control settings. The name "Altostrat" below is a stand-in for the name of the user's organization.



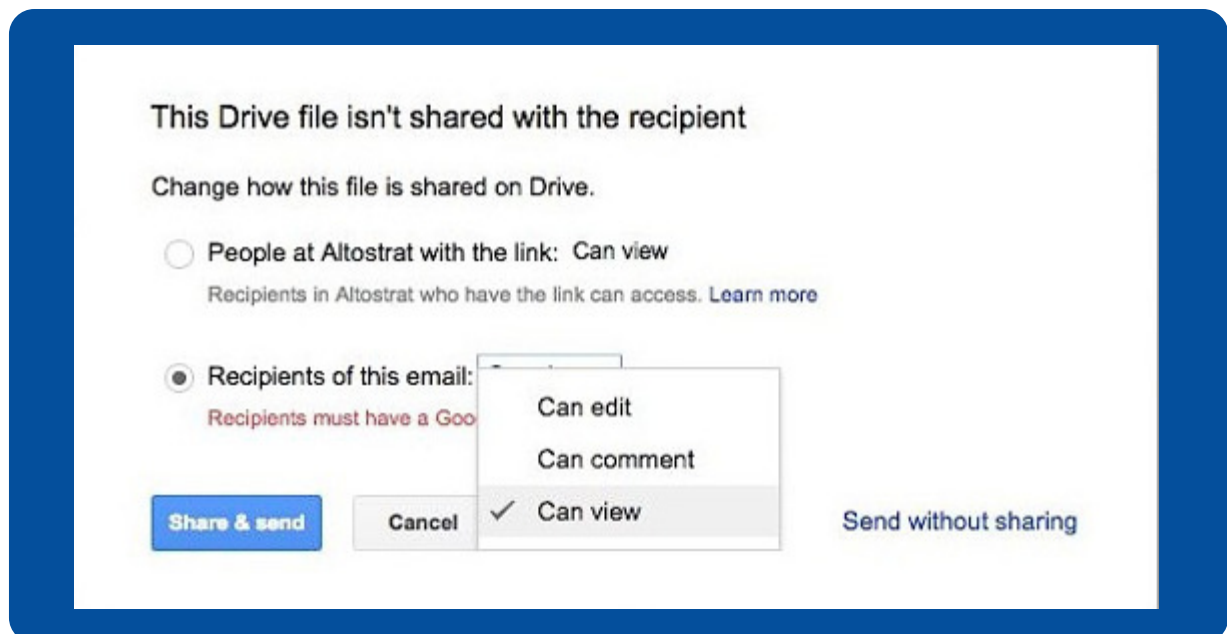
This Drive file isn't shared with the recipient

Change how this file is shared on Drive.

People at Altostrat with the link: **Can view** ▼

[More options](#)

Share & send Cancel [Send without sharing](#)



This Drive file isn't shared with the recipient

Change how this file is shared on Drive.

☐ People at Altostrat with the link: **Can view**
Recipients in Altostrat who have the link can access. [Learn more](#)

☒ Recipients of this email:
Recipients must have a Google account

Can edit
Can comment
✓ Can view

Share & send Cancel [Send without sharing](#)

HIPAA Compliant Gmail for Patient Communication

Gmail currently does not have safeguards in place to protect outgoing transmissions of PHI. That means that sending a patient PHI over Gmail will constitute a HIPAA violation if you don't have a solution in place to remedy that.

By implementing these two safeguards with the help of an IT specialist and HIPAA compliance expert, you may be allowed to send PHI to patients external to your organization's G Suite without breaking the law.

- **Encryption:**

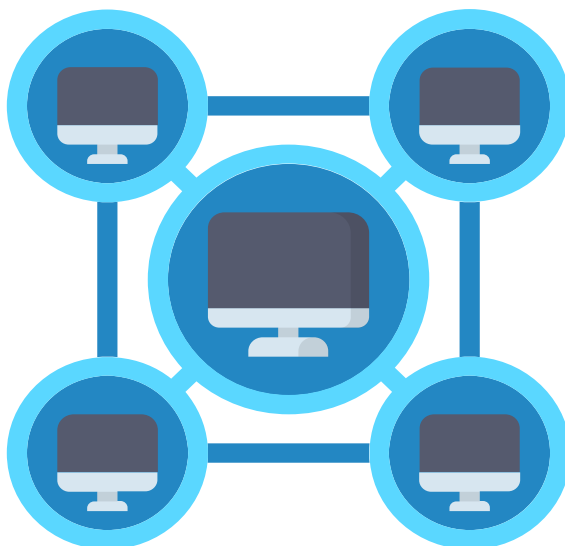
If your organization has end-to-end encrypted email and your patients understand how to access data sent to them in this manner, you may be allowed to legally send it.

AND

- **Use and Disclosure:**

You must include a provision in your organization's Use and Disclosure form asking patients for permission to send their PHI via email.

Consult an IT security provider or HIPAA Compliance Coach for more details.



HIPAA Compliance Simplified



HIPAA should be simple. That's why Compliancy Group is the only HIPAA software with expert Compliance Coaches™ holding your hand to simplify compliance. Built by auditors, Compliancy Group gives you confidence in your compliance plan, increasing patient loyalty and profitability of your organization, while reducing risk.

Why Compliancy Group?

- HIPAA Audit Support, no client has ever failed an audit!
- Total Compliance Solution
- HIPAA Seal of Compliance™
- Dedicated Compliance Coaches

This guide does not constitute legal or compliance guidance. By downloading this guide, you agree to Compliancy Group LLC's Privacy Policy. Compliancy Group takes no legal responsibility for PHI transmitted via Gmail or stored in a G Suite service.