Title: How to configure Google apps to ensure HIPAA compliance in the workplace

If you are a healthcare company and want to embrace the Google apps with which most are so familiar, you can absolutely do that, with a little bit of work and diligence. It is incumbent upon you, the healthcare organization, to properly configure your services, and you will need to work closely with your IT department to do so.

Google's products, with their built-in cloud infrastructure, provide robust security, data protection and compliance capabilities. Cloud services can be a huge benefit where data loss concerns are involved. For example, if you are a company that has in the past stored sensitive health information on company laptops, a cloud service is a much better choice for you.

Data breaches caused by stolen devices are a threat, and one that may be much higher than previously thought. According to Verizon's 2015 Data Breach Investigation Report, 45% of healthcare data breaches occur on stolen laptops.[1] With a cloud-based option like Google, sensitive data resides in the cloud, not on the laptop.

The Department of Health and Human Services (HHS) provides specific guidelines with regard to HIPAA and cloud computing solutions.[2] These will help you understand the technicalities involved in using cloud services to store or process ePHI.

In your Google app setup process, certain steps need to be taken to ensure security and privacy guidelines are being adhered to.

In order to ensure HIPAA compliance using Google apps, you must first and foremost become a paid user with Google and sign a Business Associate Agreement[3] (BAA) with them. It is important to understand that as per this agreement, PHI is only allowed in certain Google services.

---

[1] 2015 Data Breach Investigations Report, Verizon Enterprise Solutions, http://www.verizonenterprise.com/verizon-insights-lab/dbir/

[2] Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

[3] 2015 HIPAA BAA, https://gsuite.google.com/terms/2015/1/hipaa_baa.html

According to Google, “G Suite customers are responsible for determining whether they are subject to HIPAA requirements and whether they use or intend to use Google services in connection with PHI. Customers who have not entered into a BAA with Google must not use Google services in connection with PHI.”[4]

For example, services in which PHI is permitted include: Gmail, Google Drive, Google Calendar, Google Sites and Google Vault. Services in which PHI is **not** permitted include: Google Hangouts, Google Groups, Google Contacts, and Google+.[5] As such, carefully consider if or how you will use the products where PHI is not permitted.

Administrative rights should not be taken lightly or given freely. Only those who have a deep understanding of HIPAA should have said rights, and an unqualified user can be a serious problem. It is up to you in your company and within your departments to assign rights as appropriate. Perhaps only high-level IT personnel and other relevant employees with significant HIPAA training should have admin rights.

Limiting apps, and restricting user access are important for maintaining a HIPAA compliant environment. You will want to disable access to apps and add-ons from the admin console, and turn off Marketplace Apps.

With regard to Google Drive and Gmail, disable offline storage. Google Vault will come into play here. Consider adding a third-party email encryption service at this point, as well. This can improve the level of confidentiality and security of email communication with your patients, and ensure that your email has the appropriate level of encryption and protection.

Make sure that your devices are secured. The HHS guidelines clearly state that you can access your cloud service provider (CSP) data from mobile devices, "...as long as appropriate physical, administrative, and technical safeguards are in place to protect the confidentiality, integrity, and availability of the ePHI on the mobile device and in the cloud, and

---

[4] *HIPAA Compliance with G Suite*, 2017, https://support.google.com/a/answer/3407054?hl=en

[5] Google Security and Compliance Summary, November 2016, https://static.googleusercontent.com/media/gsuite.google.com/en//terms/2015/1/hipaa_implementation_guide.pdf

appropriate BAAs are in place with any third party service providers for the device and/or the cloud that will have access to the e-PHI."[6]

Auditing access within your account is a critical element, and something you will need to do on an ongoing basis. Maintaining an accurate audit trail of your PHI is absolutely essential for HIPAA compliance. The connection between your cloud storage and your devices is one that needs to be closely scrutinized, to ensure proper protection. You may want to consider disabling or restricting file synchronization where it applies to PHI, or bring in an end-to-end encryption provider to an added layer of protection.

Backup, backup, backup! As always, be vigilant about backing up your data and your Google apps. Accidental changes are made, deletions happen, and you will need to be able to recover your sensitive data. Several third party providers offer HIPAA compliant backup tools as solutions for disaster recovery.

In summary, a checklist for your Google/HIPAA configuration:

- Choose a paid plan and sign a BAA with Google
- Understand Google apps and PHI permissions
- Clearly define appropriate admins and access
- Disable apps, add-ons and Marketplace
- Disable offline storage for Google Drive and Gmail
- Consider third-party email encryption service
- Vigilantly audit account access and PHI trail
- Properly configure devices
- Restrict or disable file synchronization
- Backup your data

With the competitive nature of technology solutions today, you have a great many to choose from to meet your needs. Should you choose Google for your company and your team, rest assured that you can do safely ensuring HIPAA compliance and properly protecting the sensitive information belonging to your patients. Google provides a complete implementation guide for your reference.

---

[6] Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html