



## Google Health and HIPAA

Unlike a doctor or health plan, Google Health is not regulated by the Health Insurance Portability and Accountability Act (HIPAA), a federal law that establishes data confidentiality standards for patient health information. This is because Google does not store data on behalf of health care providers. Instead, our primary relationship is with the user. Under HIPAA, patients have a right to obtain a copy of their medical records. If they choose to use Google Health, we'll help them store and manage their medical records online.

Although Google Health is not covered by HIPAA, we are committed to user privacy and have in place strict data security policies and measures, and ensure that users control access to their information. We let users know what information we collect when they use Google Health, how we use it, and how we keep it safe. Users choose who views or adds information to their profile, and they can revoke access at any time.

There is no advertising in Google Health. We do not sell user health information, and we do not share it with other individuals or services unless a user explicitly authorizes us to do so, or in the limited circumstances described in our privacy policy. A user's personal medical records are stored in their secure account and cannot be accessed by others through a search on Google.com. Also, no personal or medical information stored in a user's Google Health profile is used to customize their Google.com search results.

The information below describes how Google Health's data confidentiality practices compare to those mandated by HIPAA.

For more information on Google Health's privacy practices, see our [privacy policy](#).

For more detailed information on HIPAA, see:

<http://www.hhs.gov/ocr/hipaa/>

<http://www.hipaadvisory.com/REGS/HIPAAprimer.htm>

	HIPAA	Google Health
<b>Do individuals have access to their medical records and health information?</b>	Under HIPAA, patients can request a copy of their medical records from their health care	In Google Health, users have free and immediate web access at all times to the

	<p>provider. This typically requires completing release paperwork and may require a printing or copying fee. In some circumstances, availability of certain records may be limited.</p>	<p>medical records and health information they store in their account.</p>
<p><b>Are individuals informed of how their information is used and protected?</b></p>	<p>Health care providers must provide patients with written notice of their HIPAA privacy rights.</p>	<p>Google provides users with a privacy policy when they sign up for Google Health.</p> <p>The policy is also posted online, along with Frequently Asked Questions, allowing users to reference it at any time.</p>
<p><b>What information is protected?</b></p>	<p>Under HIPAA, personally identifiable information is protected.</p> <p>De-identified patient information is not protected.</p> <p>Aggregate, de-identified patient information can be published and shared with third parties.</p>	<p>Under the Google Health privacy policy, personally identifiable information is protected.</p> <p>De-identified information, including our anonymous logs data, is restricted and cannot be shared with third parties.</p> <p>Aggregate, de-identified user information can be used to publish trends.</p>
<p><b>When is information sharing permitted?</b></p>	<p>Health care providers may share information with patient authorization, and may share without authorization, for certain purposes, such as:</p> <ul style="list-style-type: none"> <li>• When doctors or other health care providers share information to treat patients, like when faxing patient records for a referral</li> <li>• When used for payment, including</li> </ul>	<p>Google Health may share information with explicit user authorization, and may share without authorization in certain limited circumstances, such as:</p> <ul style="list-style-type: none"> <li>• With contractors and vendors operating solely on Google's behalf (subject to security and confidentiality requirements)</li> </ul>

	<p>sharing with insurance companies to pay for care</p> <ul style="list-style-type: none"> <li>• When employers face workplace injury claims</li> <li>• When public health researchers need aggregate information for studies</li> <li>• For health care operations, including to contractors and vendors operating on a provider's behalf (subject to security and confidentiality requirements)</li> </ul>	<ul style="list-style-type: none"> <li>• To protect against imminent harm to the rights, property or safety of Google, its users or the public, or to address fraud or violations of the Terms of Service</li> </ul>
<p><b>When is information sharing required?</b></p>	<p>Under various federal and state laws, health care providers must share patient information to comply with court orders and subpoenas.</p> <p>HIPAA itself also allows health care providers to voluntarily share patient information with law enforcement without a subpoena and without permission from or notice to the patient.</p>	<p>Under various federal and state laws, Google must share user information to comply with court orders and subpoenas. When possible, we notify the user in order to give them the opportunity to object.</p> <p>Under the Electronic Communications Privacy Act (ECPA), Google may not voluntarily share most user information with law enforcement.</p>
<p><b>How does the individual authorize sharing?</b></p>	<p>Patient authorization is not required for institutions to share information in the case of certain permitted disclosures, described above. When authorization is required, patients provide consent to share information through a written authorization form that must satisfy certain HIPAA</p>	<p>Users must request and give Google permission to share information through electronic authorization in their Google Health account. Sharing is revocable at any time.</p>

	requirements. Sharing is revocable under HIPAA.	
<b>Is information protected when used by third parties?</b>	If the third party is covered by HIPAA, HIPAA rules apply. If the third party (e.g., a patient's family member or employer) is not covered by HIPAA, HIPAA rules do not apply.	<p>If the third party is covered by HIPAA, HIPAA rules apply. If the third party (e.g., a patient's family member or employer) is not covered by HIPAA, HIPAA rules do not apply.</p> <p>Online services not covered by HIPAA that wish to integrate with Google Health must comply with <a href="#">Google Health's Developer Policies</a>, which establish strict privacy standards for how they collect, use, or share user information.</p>
<b>Can information be seen or used internally by a health care provider's or health plan's personnel or by Google employees?</b>	Employees in particular job functions may have access to patient information without patient authorization as reasonably necessary to carry out duties relating to treatment, reimbursement, or health care operations, such as to communicate about health benefit plans or to recommend alternative treatments or therapies.	A limited number of employees in particular job functions may have access to user information in order to operate and improve Google Health. Users consent to this limited internal use when they sign up for Google Health.
<b>Do individuals have a right to correct inaccurate information in their records?</b>	Patients can request corrections in their records, and the service or doctor can reject or accept the request.	Users can delete any of their health information stored on Google Health and edit any information they have entered in their account at any time, and their account will reflect their changes immediately. They can also add notes to the information sent to their account by a health care provider.

<p><b>Can individuals find out who has viewed or added information to their records?</b></p>	<p>Patients can request to see to whom their information has been disclosed in the last six years by requesting this information in writing from their health care provider. However, most disclosures, such as those for treatment, payment, and health care operations, do not have to be reported in response to such a request.</p>	<p>Every time data is added to a user's profile, the user is updated with a 'notice' on the main page of their profile. Users can see their full list of notices at any time.</p> <p>Users can view a full list of anyone that can currently view or add information to their account at any time in the settings tab of their Google Health account. This list does not include those who previously had access but from whom the user later revoked reading or editing privileges.</p> <p>Additionally, individual items that have been added to a user's account include a source--the name of the health care provider or institution that added the information--even if the source no longer has reading or editing privileges on the account.</p>
<p><b>How is information kept secure?</b></p>	<p>HIPAA requires that health care providers and other services maintain a minimum standard of "reasonable and appropriate safeguards to prevent intentional or unintentional use or disclosure of health information".</p>	<p>Google Health secures information by:</p> <ul style="list-style-type: none"> <li>• Using electronic security measures such as Secure Socket Layer (SSL) encryption, back-up systems, and other cutting-edge information security technology</li> <li>• Strongly restricting information access to a limited number of necessary personnel</li> </ul>

<p><b>Who enforces privacy protections?</b></p>	<p>Under HIPAA, the Department of Health and Human Services enforces HIPAA privacy protections through civil and criminal penalties. Read more information about <a href="#">HIPAA enforcement</a> from the HHS Office of Civil Rights.</p>	<p>Under Section 5 of the Federal Trade Commission Act, the FTC enforces privacy protections in the Google Health privacy policy through civil and criminal penalties.</p> <p>State attorneys general and district attorneys have similar authority under general consumer protection laws.</p>
---	---	---