A Platform w/ PHRs/Programs **www.google.com/health** *See FAQ for explanation of the difference between a PHR and a platform*	A	B	C	D	F	**Platform Grade = D** **Partners Grade = F** *(See Below for Grade Explanations)*
Privacy Policy/Notice:						
• Location: Privacy Policy must be easy to find and accessible from the organization's home page. Should be unavoidable and accessible on any page that collects information.		✓				Privacy Policy is up front/home page. Could improve by making more visually noticeable.
• Readability: Privacy Policy must be clear, easy to understand, and at a low reading level.				✓		The Google Health Privacy Policy is generally written in a user friendly style; it is well organized and concise. However, there are contradictory and confusing statements: *"we do not sell, rent or share your information (identified or de-identified) without your explicit consent…"* BUT *"Google will use aggregate data to publish trend statistics and associations"* (no opt out) We also find the following statement vague and confusing. The Google Health policy states that you must authorize HIPAA covered entities to send information to your Google Health account and goes on to say: "*When you ask Google to send your health information to others, you will also be giving Google permission to send those certain types of health information*." Send to whom? Under what circumstances?
• Transparency: Privacy Policy is comprehensive; individuals should not have to read multiple policies to understand how their information can be used.				✓		Multi-layered policy: 5 relevant documents had to be reviewed to understand full policy. Reviewed the following: Google Health Privacy Policy, General Privacy Policy, Google Health Developer Policies, Terms of Service, Sharing Authorization Agreement. It is incredibly difficult for the average consumer to have any confidence as to <u>what policy</u> applies in <u>what circumstances</u>, for <u>what data</u>, etc. The "exceptions" to use of information without express consent are too vague/broad. **The primary caution**: How privacy is protected in the PLATFORM is generally a higher standard than how PARTNERS protect privacy once you share your information. The sharing policy should be clearer, especially about those partners that only comply with HIPAA. HIPAA-compliant Partners can use your information without your consent. Regardless of whether a Partner complies with HIPAA, consumers need to read <u>every</u> Partner's privacy policy and terms of use before sending information from Google Health to a Partner. Google Health does provide links to these policies when you click on the Partner for a description of the service (before you add them).

Patient Control/Choice:						
• Consent for Identifiable Data: No information is shared or collected without explicit, informed consent. Privacy Policy states how information will be shared and, ideally, how it will NOT be shared.			✓ **The Google Health Platform**		✓ **Partners that can access info if you share your account**	**PLATFORM:** Google Health states up front that "*you are in control of your information.*" As a Platform, Google Health's Platform Policy requires explicit consent to share identifiable information. However, there are conflicting and vague statements in the privacy policies as noted in the section on Transparency; these confuse the commitment to obtaining "explicit consent." Google Health can also access/disclose PHI under the following circumstances: 1) to comply with law/legal process served or "enforceable governmental request" 2) to enforce terms of service 3) to detect, prevent, or otherwise address fraud, security or technical issues 4) to protect personal safety and welfare under urgent circumstances. Most of these exceptions are standard business practices. The 3rd item is far too broad. Can Google conduct fraud investigations without your consent for an insurance company or a government agency? Any access to users' information to address fraud should only be permitted if ordered by a court of law. **PARTNERS**: Take caution with Partners that are granted access to your account. The Google Health Developer Policy requires explicit opt in for sharing data. However, we have at least two concerns: 1) During our assessment, we signed up for an account and added random, multiple Partner applications. At least two of the Partners on Google Health DO NOT COMPLY with the Google Health Developer Policy. For example, TrialX, a list and matching service for research and clinical trials does not inform the user when creating an account that their information will be used for research purposes nor does it require users to agree to their privacy policy. FYI: one of the "research" projects includes an online marketing survey for people with HIV. EPillbox, another Partner, does not require the user to agree to their privacy policy. If Google Health does not systematically enforce their own Developer Policies, how can individuals trust other Google Health policies? 2) In spite of what the Privacy Policy states about consent, if the Partner is a HIPAA covered entity, or is "compliant" with HIPAA, then HIPAA applies – no questions asked. The HIPAA exception is highly problematic: any partner that operates under HIPAA is allowed to use your health information for "treatment, payment or healthcare operations" ***without getting your express consent***.
• "De-Identified Data": No de-identified or aggregate data is used without explicit, informed individual consent.					✓	Google Health uses aggregated data in many more ways besides analyzing website use. For example, data is used to publish trend statistics and associations. Google gives multiple assurances that this data cannot personally identify an individual – that is simply false. Data is anonymous or useful, never both. There is ***no way*** to opt out of any of the aggregate use of your health information on Google Health. What if Google analyzes and publishes trends about searches on drug use such as Medical marijuana? Meth? Guns? Obesity? Combined with other data sets including the increasingly sophisticated mapping technologies, you can and will be re-identified.

• Segmentation: Patients can segment/hide sensitive information.					✓	Does not appear that you can segment at any level; we shared a profile with another individual and access to the entire profile was sent.
Access/Participation:						
• Patients can easily find out who has accessed or used their information.		✓ **Platform**		✓ **Partners**		Audit trails feature is clear, easy to understand (for platform only). You can see who has accessed your information as well as a history of access, i.e. what they did and when. PARTNERS: Once your information goes out of Google Health or is shared with a Partner, how that information is accessed may or may not be tracked by that Partner.
• Patients must be able to promptly and permanently remove themselves and their health information from the system upon request.		✓ **Platform**		✓ **Partners**		Can "*completely delete at any time*" without assistance. Back up copies exist for up to 30 days. PARTNERS: If a Partner receives information from your Google Health account the Developer Policy requires them to allow permanent deletion; "back up copies may exist for a short time." This is a good requirement but we have real concerns as to whether the policy is enforced or not (see "Patient Control" criteria).
Integrity/Security:						
• Patients can expect their data to be secure. Data should only be stored in the U.S. and use authentication that goes beyond username and password login.				✓		Google Health data is stored with all other data such as gmail, calendars, etc. in the same cloud. Data is stored in the U.S. as well as other *unnamed countries*. They do use electronic security measures such as Secure Socket Layer (SSL) encryption, back-up systems.
Customer Service/Enforcement:						
• Patients can easily report concerns and get answers.				✓		May submit comment via webform and mail. We submitted an inquiry via the webform on 11/5/09 and as of 12/01/09 have not received a response.

View Google Health's entire privacy policy. We highlighted sections of importance.
www.patientprivacyrights.org/GoogleHealth_Privacy_Policies

Letter Grade	Numerical Value	Explanation
A	4.0 - 5.0	Excellent: No invasive practices; solid protections; ensures your privacy rights; user friendly
B	3.1 - 3.9	Fairly comprehensive efforts and protections, room for improvement
C	2.6 - 3.0	Some safeguards, a number of key flaws, weak protections
D	2.0 - 2.5	Few, if any, safeguards and protections, and/or misleading information, and/or very user "un-friendly."
F	1.0 - 1.9	Threatens patient privacy and control over personal information either via inaction or actual business practices

Google Health's Numerical Platform Grade
2.5

Partners Numerical Grade
1.75