A Platform with PHRs/Programs **www.healthvault.com** *See FAQ for explanation of the difference between a PHR and a platform*	A	B	C	D	F	**Platform Grade = B** **Programs 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 highlighted graphically, featured at the top of screen, links at bottom of page as well. There is a simple summary of the Platform's policies featured on the homepage with a link to the details. These summaries (provided they are true and accurate) are a helpful indicator of the importance the company places on health privacy.
• Readability: Privacy Policy must be clear, easy to understand, and at a low reading level.		✓				Generally written in a user friendly style. Most statements are straightforward; declarative.
• Transparency: Privacy Policy is comprehensive; individuals should not have to read multiple policies to understand how their information can be used.			✓			Privacy Policy is comprehensive, generally contained in one document with the following exceptions: There is a link to Microsoft's General Privacy Policy to explain Windows Live ID credentialing. There is also a link to the Service Agreement. (Note: the Liability Limitation clause makes clear that you cannot recover any damages because the account is free.) We like the commitment made here: "*We use personal health information collected through the service, including health information, to provide the Service, and as described in this privacy statement. We do not use or disclose your information except as described in this privacy statement.*" HealthVault should not be using information in any way that is not explicitly described in this policy. Unlike Google Health, there is no standard program agreement or Developer policy readily available. While this means you do not have to read multiple policies, it is difficult to know what exactly each individual program is required to do. **The primary caution:** How privacy is protected in the PLATFORM is generally a higher standard than the practices of HealthVault's PROGRAMS. The policy should be clearer about this, especially about those programs that only comply with HIPAA. HIPAA-compliant programs can use your information without your consent. Regardless of whether a Program complies with HIPAA, consumers need to read <u>every</u> Program's own privacy policy and terms of use before sharing any information from HealthVault.

						HealthVault encourages you to examine the terms of use and privacy policies of all programs. They do not provide links to these policies, however, until you click on "Add". This information should be provided up front with the description of the service. Later in the process, when you're about to add the service, a link should also be provided.
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 Health Vault platform**				✓ **Programs that can access info if you share your account**	**PLATFORM:** HealthVault states up front that the individual is in control of their information on the Platform. Your records are not used or disclosed without your consent. You decide who to share your account with. Health Vault can access/disclose PHI under the following circumstances: 1) comply with law/legal process served 2) protect and defend rights or property of Microsoft 3) urgent circumstances to protect personal safety and welfare These exceptions are fairly standard business practices. We would have much greater concern if these clauses were broader. **PROGRAMS:** Take caution with the Programs that are granted access to your account. Programs are required by HealthVault to "*protect privacy*" and all Programs must not "*disclose your data without express consent…*" However, there are at least two concerns: 1)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.*** 2) During our assessment, we signed up for an account and added random, multiple Program applications. In general, the 'non-HIPAA' Programs we reviewed would not share information without consent. However, one Program randomly selected, OneTouchZoom, states that when you use their site, you consent to their terms. That is not express or informed consent. They also "*combine [personally identifiable information] with other actively collected information...*" and may "*disclose your personally identifiable information you provide via this site to Johnson & Johnson affiliates worldwide...*" We don't think this policy offers the privacy protections HealthVault states it requires.
• "De-Identified Data": No de-identified or aggregate data should be used without explicit, informed individual consent.			✓			Microsoft uses aggregate data for evaluating the website and some marketing analysis. You cannot opt out of this practice.

• Segmentation: Patients can segment/hide sensitive information.		✓				When you share information in your account, HealthVault allows you to decide if others can view only, view and modify, share with others, see only specific pieces and set a time limit for access. You can decide what types of information you share (medications, conditions or diagnoses, heart rate, allergies). This works very well when sharing with other individuals or doctors' offices. You are not able to segment information at this granular level when you share information with a Program. If the consumer could dictate to the program exactly what information they share we'd give this feature a strong"A". Your only option if you do not want to share certain requested information with a Program is to not add or use that Program.
Access/Participation:						
• Patients can easily find out who has accessed or used their information.		✓ **The HealthVault Platform**		✓ **Programs**		The audit trails feature is clear and easy to understand (for platform only). PROGRAMS: Once your information goes out of HealthVault or is shared with a program, how that information is accessed may or may not be tracked by that Program.
• Patients must be able to promptly and permanently remove themselves and their health information from the system upon request.		✓ **The HealthVault Platform**		✓ **Programs**		You can delete a record without assistance. If an account was shared with others it is removed from their view after deletion; after 90 days the files are permanently deleted. PROGRAMS: if you send information from HealthVault to a program, you must ask that Program to delete the information. Programs' policies may be different than HealthVault's policies on deletion and retention.
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.			✓			Information stored on servers with limited access in controlled facilities in the U.S. All communications, except email are encrypted.
Customer Service/Enforcement:						
• Patients can easily report concerns and get answers.		✓				Customer service available via email, webform and mail. Also can contact TrustE with a complaint. We submitted an email inquiry through the webform and received a response the same day.

View HealthVault's entire Privacy Policy. We highlighted sections of importance.
www.patientprivacyrights.org/MS_HV_Privacy_Policy

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

Microsoft HealthVault's Numerical Grade
3.9

Programs' Numerical Grade
1.75