Microsoft HealthVault and Data Protection Requirements

Following is a brief explanation of how the HealthVault platform works, in relation to the European Data Protection Directive 95/45/EC and similar national laws.

1. Microsoft HealthVault accounts hold individuals' personal health records.
Microsoft offers HealthVault accounts to individuals as a free service, to collect their own health-related information from a variety of sources and store, manage, share and control it themselves. A HealthVault account offers:

- an online storage facility for consumers to keep health-related information; and
- a set of features consumers can use to collect, view, share, and transfer health-related information.

HealthVault accounts are intended for users' personal and family affairs. Users are always free to choose what data to store in their records, and whether to share or exchange data with other people or applications. We expect users to choose a variety of connections for their records, not to use them for a single health-related relationship. You can see examples of programs users may select at www.healthvault.com apps and devices directory.

Microsoft processes users' data according to the service agreement and privacy statement for the account. You can review the HealthVault account terms at

- www.healthvault.com/legal and
- www.healthvault.com/privacy.

As part of HealthVault account signup, users explicitly consent to Microsoft processing their health data.

2. HealthVault does not offer record storage on behalf of other organisations.

The HealthVault platform service offers:

- organisations a set of features they can use to offer their customers or patients (users) the ability to send and/or receive information using their personal HealthVault record; and
- users the ability to choose data transfer connections for their HealthVault record, including the ability to terminate those connections at any time.

Organisations can use HealthVault platform services to connect an application or web portal to HealthVault. They can allow their users to transfer data between the system they operate and the HealthVault account that the user controls. Before an organisation can add any information to a HealthVault record, the user must have first:

- created a HealthVault account by agreeing to a contract and privacy terms that clearly show Microsoft is directly responsible for operating and safeguarding the user's records; and
- explicitly authorized connectivity between the HealthVault record and the organisation's system (including a list of the types of data that may be included in any exchange, and whether data can be read, written, or both).

HealthVault is an additional way for organisations to transfer health information to customers or patients, replacing or supplementing mail, fax, DVD, and similar methods. Because systems cannot send data to a HealthVault record until a user authorizes the connection, transfers to HealthVault are always with user consent. However, depending on local expectations, organisations may wish to consider adding their own authorization process in their application or services.

HealthVault record-holders will deny access if they do not wish to receive their copy of information this way. They can later terminate the organisation's data access at any time. Users can continue to maintain their HealthVault records regardless of whether they choose to connect or disconnect the organisation's application.

HealthVault users can add, change or delete information in their records, and can terminate an organisation's access. As user-controlled records, HealthVault is not intended for, and not offered for use as, part of an organisation's product, service or data storage. If an organisation wants to include any of the data that a user stores in HealthVault in its records, the organisation should put a copy in its own, separate storage system.

3. Data control and processing.

The laws of the E.U. and many countries are intended to ensure that citizens can control the use and disclosure of information about themselves. HealthVault is designed to provide users with control over their personal information, flexible choices for how to use and share it, and the ability to maintain their health records independent of any particular healthcare provider. It is Microsoft's view that:

- Microsoft processes data to provide services to data subjects and their authorized representatives, under the HealthVault account terms.
- Microsoft and organisations that operate connected applications do not process data on each others' behalf; they each process data for their respective users.

A contract is required before an organisation can connect its application with any HealthVault record. Microsoft requires certain minimum security and privacy commitments in the agreement, for a reasonably consistent and informed experience when HealthVault users decide whether to connect their records with an application. The agreement recognizes that each party has a duty to protect the privacy, security and integrity of its users' data. Microsoft does not approve providers' privacy notices or generally review their practices, but does reserve the right to suspend or terminate connectivity if we become aware they may not be not fulfilling their privacy and security commitments to users.

Because Microsoft and application providers are independent service providers that both have direct agreements with their users, data processor terms (such as standard clauses adopted by the European Commission) do not apply to the agreement.

4. HealthVault data use and transfer

Microsoft does not access health data in a user's account except as necessary to operate the service and as described in the HealthVault Privacy Statement. Except for the limited circumstances described in the privacy statement, Microsoft only discloses or transfers data based on the user's active choice to establish a specific connection with their HealthVault record.

Users can close their accounts or delete information at any time.

5. Geographic location

As of the date of this paper, HealthVault records for accounts offered outside the U.S. are stored in England. HealthVault is supported by U.S. personnel, who may access data to the extent required for operational purposes.

Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Economic Area, and Switzerland https://safeharbor.export.gov/list.aspx. Microsoft informs users that their data in HealthVault may be processed in the United States or other countries where Microsoft or its affiliates, subsidiaries or service providers maintain facilities.

Organisations may have concerns about law enforcement access to data held in HealthVault. The USA PATRIOT Act (Patriot Act) is a focal point for these concerns, since it has been reported to broaden the U.S. government's ability to access data held by cloud service providers. The Patriot Act is targeted legislation focused on strengthening the ability of the U.S. Government to combat terrorism. Most countries, not just the U.S., assert jurisdiction outside their territory in some circumstances. Unless a user's data relates to terrorism or clandestine intelligence activities directed at the U.S., the Patriot Act is unlikely to be relevant. U.S. laws — including those that were amended by the Patriot Act — provide multiple levels of privacy protection for individuals, including data stored in the cloud. These laws place important process and substantive limitations on the U.S. government's ability to require cloud service providers to disclose a user's data, regardless of their citizenship. Because Microsoft adheres to the EU-U.S. Safe Harbor Agreement, the Patriot Act has no effect on our compliance with the Data Protection Directive.

5. Microsoft's approach to privacy and security

Microsoft designs and operates HealthVault based on corporate policies developed over years of attention to privacy and security issues, influenced by input from experts and advocates. For example, HealthVault accounts include history where the account-holder can see the source, any changes, and who has viewed data in the record. Health data in HealthVault is encrypted both in storage and when transmitted between HealthVault and connected applications.

We expect HealthVault features to evolve as we learn more about the needs of our users. We are committed to providing our users with clear and understandable information about the choices they can make in storing, sharing, and transferring their health information using HealthVault. Microsoft works collaboratively with agencies and stakeholders that develop privacy and security rules and standards, because we believe that effective privacy protections that establish trust are critical to the success of health IT and health care in general. Some recent examples of Microsoft engagement in privacy issues can be found at http://www.microsoft.com/privacy.