Microsoft HealthVault, HIPAA and HITECH

Potential HealthVault platform customers in the U.S. often wonder how the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act relate to HealthVault. As a brief explanation:

1. Microsoft HealthVault accounts hold individuals' personal health records.

HealthVault accounts are a service offered to individuals, 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.

Microsoft offers HealthVault accounts directly to individuals for personal use, and not for or on behalf of covered entities. We expect users to choose a variety of connections for their records, not to use them for a single healthcare relationship. You can see examples of programs users may select at www.healthvault.com apps and devices directory.

We operate HealthVault according to the commitments we make to HealthVault end users in our service agreement and privacy statement. As such, HealthVault records are personal health records as defined in the HITECH Act.

2. HealthVault does not offer records as part of covered entities' electronic health records.

The HealthVault platform service offers:

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

Covered entities can use HealthVault platform services to connect an application or web portal to HealthVault. They can allow their patients to transfer data between the system operated by the covered entity and the HealthVault account that the patient controls. Before a covered entity can add any information to a HealthVault record, the record-holder must have first:

- created a HealthVault account after reviewing legal 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 covered entity'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 record-holders will deny access if they do not wish to receive their copy of information this way. They can later terminate the covered entity's data access at any time. Patients can continue to maintain their HealthVault records regardless of whether they choose to connect or disconnect the covered entity's application.

As consumer-controlled records, HealthVault is not intended for, and not offered for use as, part of a HIPAA covered entity's electronic health record. HealthVault account holders can add, change or delete information in their records, and can terminate a covered entity's access. If a covered entity wants any of the data that a user stores in HealthVault included in the electronic health record, it should put a copy in its own, separate, electronic health record system.

You can review the HealthVault account terms at www.healthvault.com/legal and www.healthvault.com/privacy.

3. Information transfer to records

HealthVault is an additional way for HIPAA covered entities to transfer health information to patients, replacing or supplementing mail, fax, DVD, and similar methods. You should consult your legal advisor about any requirements applicable to such transfers. The HHS Office for Civil Rights has also made a useful explanation of PHRs and the HIPAA Privacy Rule available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

4. Platform customers that are HIPAA covered entities have an option to sign the HealthVault business associate agreement.

HIPAA regulates the flow of health information when it is out of the patient's direct control—for example, when a healthcare provider forwards it to third-party billing services. At the same time, HIPAA clearly recognizes that patients have a right to a copy of their own health information. It includes an explicit mechanism to allow patients to receive copies on request.

Microsoft operates HealthVault according to the commitments we make to end users in our service agreement and privacy statement. As such, for U.S. users, the Federal Trade Commission regulates security and privacy of HealthVault records. For example, we would manage any breaches of U.S. HealthVault user data according to the FTC's Health Breach Notification Rule. Microsoft cannot agree to report to covered entities about information sent to HealthVault records, as required by business associate agreements, because of our privacy commitments to HealthVault account-holders.

However, some covered entities see ambiguity and uncertainty in health privacy requirements. We do not want this uncertainty to stall progress toward a dynamic, trusted, patient-centric health care system. That is why we offer HealthVault platform customers that are HIPAA covered entities the option to sign our HealthVault business associate agreement.

The HealthVault business associate agreement excludes information that is in a HealthVault account. Therefore, it is not likely to be relevant to HealthVault platform operations, but we understand that some customers may find it worthwhile as additional evidence of our commitment to security and privacy in transmission of data.

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. 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 at www.healthvault.com/privacy.

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. Effective privacy protections that establish trust are critical to the success of health IT and health care in general.