

**Written Testimony of
Michael Stokes
Principal Program Manager, Microsoft Corporation's Health Solutions Group
Before the
Senate Judiciary Committee
Hearing on Health IT: Protecting Americans' Privacy in the Digital Age
January 27, 2009**

Chairman Leahy, Ranking Member Specter, and distinguished members of the Committee, my name is Michael Stokes, and I am a Principal Program Manager in Microsoft's Health Solutions Group. In this role, I focus on privacy issues, and I very much appreciate the opportunity to share Microsoft's views on the importance of privacy and health IT. We commend the Committee for holding this hearing today and for your efforts at the intersection of privacy, information technology, and healthcare reform. We are committed to working collaboratively with you, the Department of Health and Human Services, the Federal Trade Commission, consumer advocates, and other stakeholders to protect the privacy of health data.

Microsoft is here today because we are deeply engaged on both health IT and privacy issues. Over 12 years ago, Microsoft began developing technologies focused on the health industry, with the goal of using software and the Internet to transform healthcare, as they have so many other industries-- opening new ways of working, new ways of communicating, and new economics. Our products, including HealthVault for consumers and Amalga for hospitals and health systems, are focused on driving scalable health IT solutions that can benefit all.

Microsoft also has a deep and long-standing commitment to privacy. We recognize that consumers will only be comfortable sharing their information if they trust that they will have control over its use and know that it will be protected. Establishing trust is especially important with respect to health data. This is because of the important role that health data plays in our overall healthcare system. Delivering quality, reliable healthcare requires that data be shared. New therapies, new cures, and new lessons about disease will be driven by the availability of health data. By working together to encourage data liquidity through strong privacy protections, we can realize the value of data sharing and thereby drive real change in our healthcare system.

Today, I want to discuss how we can promote the widespread use of innovative health IT solutions and the sharing of health data while still protecting privacy. My testimony today begins by describing what we believe to be the future of healthcare--a totally connected environment where patients and providers trust each other and use health IT to share information seamlessly. It then discusses how the three components of trust--transparency, control, and security--can provide flexible technology solutions that improve our current healthcare system. It concludes by showing how the same

principles of transparency, control, and security underlie Microsoft's approach to privacy in health IT.

I. The Future: Dynamic, Trusted, Consumer-Driven Healthcare

There has been much discussion and debate about how to improve the healthcare system in the United States. But we think it is fair to say that we all have a single goal in mind: to deliver predictive, preventive, and personalized medicine in an accessible, affordable, and accountable way. In our view, health IT and privacy are necessary elements to achieve this success.

A. Health IT Can Build a Patient-Centric System The future of medicine and improvements in our healthcare system depend on the seamless exchange and reuse of health data. Today, in order to manage their health, consumers must deal with both paper documents and electronic files. Few people have the resources to keep track of medication lists, vaccination histories, appointment calendars, lab results, diet plans, exercise schedules, and all the other components of health data. Most people have little knowledge of how to prevent disease and little, if any, support for managing their healthcare.

What if consumers could collect all their health and wellness data electronically, could keep it securely stored in one place over time, and could share relevant elements of this record securely from provider to provider, no matter the doctor or insurance company with whom they interact? With all the relevant data at their fingertips, accessible at any time and any place, they could sign up for services that provide personalized alerts and information. They could track fitness goals across numerous devices, such as exercise bikes that monitor vital signs, smart watches that record the number of miles run, and scales that measure body fat as well as weight. They could research relevant medical conditions online and interact with support groups so that they would be better prepared and informed for their next visit to the doctor. And they could share data with their support systems and make better health decisions for themselves and their families.

A patient-centric system would benefit healthcare professionals and hospitals as well. Today, patients often see multiple doctors, often spread across multiple health systems. Each doctor sees only a fragment of the patient's health data, which can lead to unsound medical decisions and excessive costs. Health IT can connect an individual's existing data, allowing healthcare professionals to see a complete picture of their patient. This will enable providers to eliminate unnecessary procedures, avoid harmful drug interactions, and concentrate on providing better quality care.

At Microsoft, we believe technology can make this vision a reality without sacrificing privacy protections. We envision a healthcare ecosystem that places patients at the center of a protected and connected network, with:

1. Patients as consumers--experiencing more control, more convenience, better service, and ultimately better value for what they spend on healthcare.
2. Physicians as knowledge workers--professionals getting the right data in the right format at the right time to provide the best treatment and preventive care.
3. New interactions among the key members of the healthcare ecosystem--physicians, patients, pharmacies, researchers, and insurance providers benefiting from a new flow of data to make better, faster decisions.
4. The extension of modern healthcare to the virtual space--patients getting care when they want it, wherever they need it, thanks to virtual medical clinics, virtual doctor visits, virtual lab results, medical homes, and personalized medicine based upon genomic data.
5. A learning healthcare system--one that measures key data points, identifies errors, and makes improvements in order to deliver value.

In this new healthcare system, everyone will have the right information at the right time with computer assisted decision support, enabling the seamless exchange and reuse of data. Health data is the asset that will drive an efficient, high-quality, value-based, evidence-focused future for medicine, achieving one of the priorities of Congress and the new Administration.

B. Trust Is Essential to a Patient-Centric Healthcare System

Health data is the fuel that will drive a connected, patient-centric healthcare system. It is therefore critical that consumers, providers, and other participants in the healthcare ecosystem be willing to share health data. To facilitate such sharing, we must establish a foundation of trust.

Health data is often considered more sensitive than other personally identifiable information. If health data is stolen or lost, it is not simply a matter of recovering financial assets. It can impact an individual's employment, ability to receive healthcare, and social standing. And the effects are not limited to the individual whose data was lost, because health data may also be relevant to the person's children, grandchildren, or distant relatives. Indeed, there is evidence that many Americans do not actively participate in their own healthcare due to privacy concerns:

1. According to the Department of Health and Human Services, two million Americans with mental illness do not seek treatment for this reason.
2. Approximately 600,000 cancer victims do not seek early diagnosis and treatment.
3. Millions of young Americans suffering from sexually transmitted diseases do not seek

diagnosis and treatment (1 in 4 teen girls are now infected with an STD).

4. The California HealthCare Foundation found that 1 in 8 Americans have put their health at risk by engaging in privacy-protective behavior: avoiding their regular doctor, asking a doctor to alter a diagnosis, paying privately for a test, or avoiding tests altogether.

5. The Rand Corporation estimated that 150,000 soldiers may be suffering from Post-Traumatic Stress Disorder (PTSD), many of whom do not seek treatment because of privacy concerns

Because health data can be highly sensitive, consumers and healthcare providers will only share such data if they trust that the privacy of health data will be protected. When such trust is established, data will flow freely, benefiting all participants. Consumers will receive better information about appropriate treatments, medications, nutrition, and exercise. Healthcare providers will receive more reliable health data and greater patient compliance, which in turn leads to better quality care and improved cost efficiencies both for treatment of individual patients and for public health purposes. In short, effective privacy protections are critical to the success of health IT and healthcare in general.

II. Trust Requires Transparency, Control, and Security

Transparency, control, and security are necessary to help ensure that consumers and healthcare providers trust, and are willing to participate in, the healthcare system.

A. Transparency Can Help Stakeholders Understand How Their Data Is Used

Transparency is significant because it provides consumers with an informed understanding of a company's data collection practices, of how their data might be used, and the privacy controls available to users. Without transparency, consumers are unable to evaluate a company's services, to compare the privacy practices of different entities to determine which products and services they should use, or to exercise the privacy controls that may be available to them. Transparency also helps ensure that when consumers are dealing with a company that has adopted responsible privacy practices, consumers do not needlessly worry about unfounded privacy concerns that might prevent them from taking advantage of new technologies.

Transparency is especially important with respect to healthcare data. If patients do not understand what data is being collected, who has access to the data, and what the data will be used for, they may decide not to provide the information at all--not even to their treating physicians. Without this data, doctors will not be able to make fully informed treatment recommendations, and overall consumer health could suffer.

Providers need transparency too. They need to understand how the health data they make available to patients and others may be used; they need to know whether such data may be disclosed to third parties; and they need to feel comfortable that health data will be protected.

Transparency is also essential to ensure accountability. Regulators, advocates, journalists, and others have an important role in helping to ensure that appropriate privacy practices are being followed. But they can only examine, evaluate, and compare practices across the industry if companies are transparent about the data they collect and how they use and protect it.

B. Control Can Help Stakeholders Manage Their Data Effectively

Transparency by itself is not enough. Stakeholders also need control over where their data is, who is looking at it, and for what purpose. For example, control allows patients to decide when and under what conditions they want to receive alert services or medical information that might be relevant to them. And if providers can control where health data is going, they will be better able to comply with applicable laws, regulations, and policies.

Control is particularly important when the consumer or provider needs a proxy to guide his or her choices. Patients often need to share data with custodians, guardians, or family members, but they may want to ensure that the data is only shared under certain conditions (e.g., only when the patient is unable to make decisions for himself) or only for certain periods of time (e.g., only data about the past year rather than the patient's entire lifetime). Similarly, physicians often rely on nurses, staff, specialists, and laboratory technicians to provide care for a patient. Access controls can help ensure that the patient's health data is shared only with the healthcare professionals who need to see it, and that the patient's data is not inadvertently misplaced or deleted.

At the same time, however, control should not impede the flow of clinical data that healthcare professionals need to provide effective care. For example, some members of the healthcare community have pointed out that a system requiring repeated patient consents for the disclosure of clinical data could potentially hamper treatment in situations where care must be coordinated among multiple physicians. We all need to work together to create an environment that facilitates rather than hinders care.

C. Security Can Give Stakeholders the Confidence to Adopt Health IT Innovations

Concerns about the collection and use of personal data, widely publicized security and data breaches, and growing alarm about healthcare fraud and identity theft threaten to erode public confidence in digital health solutions. Cybercriminals are increasingly exploiting personal data to make a profit, and there are a growing number of security attacks that target personal data. A recent report from the Department of Health and Human Services noted that medical identity theft can lead to patients receiving the wrong care because of inaccurate data on their health records, being blocked from receiving health insurance or other benefits, or incurring financial obligations for services that were never provided.⁶

Security helps ensure that patients and providers do not spend time and resources dealing with data breaches, identity theft, and security flaws. Once stakeholders feel confident that their data is secure, they will be more willing to adopt the innovative health IT solutions that can improve care and reduce costs. Moreover, health IT can also improve security. For example, technology that verifies patients' identities, monitors access to health records, and identifies anomalies in services requested could help prevent and detect medical identity theft.⁷

D. Transparency, Control, and Security Provide Flexible Privacy Protections

Privacy protections are not just about patients. Doctors have data of their own that they want to keep private. Additionally, hospitals, insurance plans, research facilities, and other healthcare organizations are major businesses that need to protect their intellectual property and trade secrets. Transparency, appearance of treatments for chronic conditions not previously diagnosed; increases in prescriptions that may indicate drug-seeking behavior; or attempts to receive care at multiple locations, all remote from the individuals' residences").control, and security protect privacy in ways that are flexible enough to accommodate all stakeholders in the healthcare system, not just consumers.

Moreover, today's healthcare ecosystem consists of a complex mixture of legacy and new, innovative solutions. Retrofitting existing systems may require significant design changes, and it may not be viable for everyone to upgrade their technology systems. One potential path forward is to provide a combination of simpler, less flexible, baseline solutions and newer, more complex, extensible technologies that encourage migration toward a more privacy-protective future. Following the principles of transparency, control, and security enables participants to provide privacy protections that are flexible and vibrant enough to support all of these technical solutions and business models.

III. Microsoft's Efforts to Build Trust Through Transparency, Control, and Security

Microsoft or anyone that provides tools and technologies involving healthcare data must adopt strong privacy practices that support trust. If people feel that the privacy of their healthcare data is not being protected, they will make less use of healthcare information technologies, which can hurt them and the healthcare industry alike.

Microsoft has been deeply engaged on privacy issues. Microsoft was one of the first companies to appoint a chief privacy officer, an action we took nearly a decade ago, and there are now several hundred employees throughout the company who focus on privacy as part of their jobs. We have a strong set of internal policies and standards that guide how we do business and how we design our products and services in a way that respects and helps protect user privacy. And we have made significant investments in privacy training and in building our privacy standards into our product development and other business processes.

A. Transparency by Providing Clear Disclosures

Microsoft is committed to providing transparency in its products and services. One example is HealthVault, Microsoft's free Internet-based platform that allows consumers to store copies of their health records, upload data from home health devices, share data with healthcare providers, and access products and services to help improve their health. HealthVault's privacy statement is designed to be easy to understand. We have eliminated passive language, and we wrote the statement at a high-school reading level. We also organized the privacy statement in terms of a consumer's perspective on how to use the HealthVault service, much like an abbreviated help document. We use third-party seals such as TRUSTe and eHon, we ask advocates and regulators to review our policy before launches and major revisions, and we encourage users to provide feedback.

Moreover, the HealthVault network currently has 40 live applications--programs that can connect with HealthVault, such as personal health records and alert services. Some of these applications are provided by Microsoft's partners. Before any application is authorized to access a consumer's data, we make sure that the consumer knows which application is requesting the data, what data is being requested, what the data will be used for, and which data elements are required or optional. HealthVault also stores audit trails, so that consumers can see who has accessed their health records and what actions have been taken.

B. Control by Offering Granular Access

Microsoft has made user control a key component of our healthcare solutions. We provide many different tools to help users control how their data is accessed and used. For example, in HealthVault, consumers can control what type of data is shared, who else has access to that data, whether others are allowed to modify or only to view the data, and how long others can access the data. These tools give consumers the flexibility to adjust their access decisions as their health needs change, so that a consumer who is suddenly diagnosed with a serious condition can immediately start sharing relevant data with his treating physician. Moreover, consumers can designate other "custodians" who can then share access with others, enabling records to be transferred from parent to child as the child reaches maturity or from elderly parent to adult children for extended care.

We have also implemented control features in our other health IT products. For example, just under a year ago, we launched Amalga, our family of enterprise data sharing and intelligence solutions, which connect a hospital's or health system's existing legacy systems and any new systems. This allows patient data to be viewed and queried holistically, enabling a shift from departmentally focused systems to more patient-centric systems. Amalga includes controls that allow hospitals and health systems to determine which data is shared when and with whom.

C. Security by Following Comprehensive Best Practices

Security has been fundamental at Microsoft for many years as part of our Trustworthy Computing initiative, and we have taken a broad approach to protecting the security of personal information. This approach includes implementing technological and procedural protections to help safeguard the information we maintain. For example, Microsoft has developed a Security Development Lifecycle program that calls for security evaluations and an appropriate combination of security measures, such as independent security penetration testing, independent certifications including ISO 27001, information segmentation, Lightweight Directory Access Protocol (LDAP) integration, auditing and logging capabilities, controlled-access facilities, and encrypted Internet protocols when communicating personal health data. We also have taken steps to educate customers about ways to protect themselves, and we have worked closely with industry and law enforcement around the world to identify security threats, share best practices, and improve our coordinated response to security issues.

IV. Conclusion

Microsoft recognizes that technology is only a part of a comprehensive approach needed to drive real change in our healthcare system. Education, leadership in healthcare organizations, and meaningful public policy are also critical components to success. We look forward to partnering with you and all participants in the healthcare ecosystem to move toward dynamic, trusted, and consumer-driven healthcare. Thank you for giving us the opportunity to testify today.

?

1 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,779 (Dec. 28, 2000).

2 Id. at 82,777.

3 Id. at 82,778; Press Release, Centers for Disease Control and Prevention, Nationally Representative CDC Study

Finds 1 in 4 Teenage Girls Has a Sexually Transmitted Disease (Mar. 11, 2008), <http://www.cdc.gov/STDConference/2008/media/release-11march2008.htm>.

4 California HealthCare Foundation, National Consumer Health Privacy Survey 2005 (Nov. 2005), <http://www.chcf.org/topics/view.cfm?itemID=115694>.

5 RAND Corp., Invisible Wounds of War 55, 104, 436 (2008), <http://www.rand.org/pubs/monographs/MG720/>.

6 Booz Allen Hamilton & Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, Medical Identity Theft Final Report (2009), <http://www.hhs.gov/healthit/documents/MedIdTheftReport011509.pdf>.

7 Id. at 14 (noting, for example, that IT systems can "review transactional records and detect such anomalies as the appearance of treatments for chronic conditions not previously diagnosed; increases in prescriptions that may