

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
<http://www.microsoft.com/>



March 5, 2009

The Honorable Patrick Leahy, Chairman
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Orrin G. Hatch
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Re: Written Questions Following Hearing on
"Health IT: Protecting Americans' Privacy in the Digital Age"

Dear Chairman Leahy and Senator Hatch:

Thank you for the opportunity to testify at the Senate Judiciary Committee's January 27, 2009, hearing on "Health IT: Protecting Americans' Privacy in the Digital Age." Privacy issues will continue to be important as organizations and agencies work to implement the health IT provisions in the American Recovery and Reinvestment Act ("ARRA") and to bring about real change in our healthcare system.

Microsoft believes that strong privacy protections are not only compatible with bringing the benefits of health IT to patients, providers, and healthcare organizations, but are essential to ensuring the future of the U.S. healthcare system. As my testimony emphasized, data liquidity can drive new therapies, new cures, and new lessons about disease, but patients will only be comfortable sharing health data if they feel confident that their health privacy is being protected.

This means that Microsoft, and all organizations that use or provide health IT, must adopt meaningful privacy practices that build trust with consumers. To do this, we must be transparent about what health data is collected from patients and how such data will be used; we must offer patients controls over the use and disclosure of their health data; and we must protect health data from unauthorized access.

Microsoft looks forward to cooperating with the public and private sectors to build the principles of transparency, control, and security into health IT systems, thereby establishing the trust that is critical to the success of health IT and healthcare in general.

Your follow-up questions raise interesting and important issues. Please find below our responses to the specific questions you have asked.

I. Chairman Leahy's Written Questions for Michael Stokes

1. Web-based personal health records were created to empower consumers to be more actively engaged in their own health care. This new technology enables ordinary persons to store and control their medical data on-line. Yet, serious concerns have been raised about the potential breach of privacy and security of on-line personal health records. A report issued last February by World Privacy Forum found that storing health records on-line can be counterproductive to safeguarding consumer privacy; it can open the door for sensitive health data to be easily accessible to hackers and shared by commercial data brokers outside the health care system. Your company recently launched a web-based personal health record database called HealthVault. How will Microsoft ensure that HealthVault will adequately protect individuals' sensitive health records from inappropriate access or use?

Microsoft recognizes that health data can be highly sensitive, and we are committed to protecting the privacy of that data. In HealthVault, we have implemented a series of safeguards based on the principles of transparency, control, and security.

- Transparency. HealthVault provides a clear, easy-to-read privacy notice. The notice tells users how, where, and why Microsoft uses personal data collected through HealthVault. It also explains when and why a third party might request access to personal data.
- Control. HealthVault gives individuals control over their own health records, enabling them to decide what goes into the record and who will be able to see, use, and share that data. HealthVault data is not shared with third parties unless the third party has disclosed what the data will be used for and the individual has affirmatively authorized the third party to access the data.
- Security. To protect against hacking and other illicit intrusions, Microsoft has implemented strong security measures. Our broad approach to protecting the security of personal information incorporates a wide array of technological and procedural protections, including independent security penetration testing, auditing and logging capabilities, controlled-access facilities, and encrypted Internet protocols when communicating personal health data. We have also partnered with industry, law enforcement, and consumer groups around the world to identify security threats and share best practices.

2. One of the areas of contention over health IT legislation is whether, and to what extent, patients should exercise control over the operation of their health care records. Consumer advocates tend to favor proposals that would allow consumers greater control over who accesses their information. Other stakeholders, however, contend that greater consumer control may jeopardize effective and high quality health care. What does Microsoft think about giving American consumers more control over their own health data?

For consumer services such as HealthVault, Microsoft believes in empowering consumers to be stewards of their own health data. HealthVault is based on the idea that consumers should be able to connect all their health and wellness data electronically, share it securely from provider to provider, and keep it in one place over time, no matter the doctor or the insurance company. Consumers using HealthVault already have the ability to access an audit trail that indicates who has accessed their records and what actions have been taken. When consumers understand who will be looking at their data, have control

over its dissemination, and feel confident that the data will be secure, they will be more comfortable entrusting their sensitive data to the healthcare system.

When it comes to clinical records, Microsoft provides technological tools that enable the custodian of the information to implement effective privacy controls. In enterprise solutions such as Amalga, Microsoft's software allows hospitals to comply with applicable laws and regulations and to customize their data policies as they see fit. The ARRA expands individuals' right to obtain an accounting of disclosures of their electronic health information, including disclosures for treatment, payment, or healthcare operations during the three prior years. Microsoft believes that the accounting requirement in the ARRA can be implemented in a way that provides consumers with meaningful information about disclosures of their health data without jeopardizing healthcare effectiveness, and we look forward to partnering with the public and private sectors in order to achieve this outcome.

II. Senator Hatch's Written Questions for All Panel Members

1. I strongly support health IT, but believe this must be done very carefully so that we give health care providers the proper incentives to adopt technology without increasing regulatory burdens and costs. Many health care groups have expressed concerns that requiring new and untested privacy mandates could damage the ability of providers to communicate with patients about treatment options and alternatives. They are also concerned that additional privacy requirements would add costs to the health care system, and actually discourage providers from adopting the very health IT we want them to use. Do you share these concerns and how would you recommend Congress and the Administration prevent these problems from occurring?

Microsoft agrees that privacy requirements need to be carefully designed so that they do not discourage providers from adopting health IT. Privacy protections based on the principles of transparency, control, and security can help ensure that both providers and patients trust, and are willing to participate in, the system.

In my role as Principal Program Manager for Microsoft's Health Solutions Group, I am responsible and accountable across the group for compliance with the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act ("HIPAA"). My understanding is that the HIPAA Privacy Rule and the new provisions under the ARRA still allow providers to discuss treatment options and alternatives with their patients without obtaining prior authorization to do so. Under HIPAA, communications that relate to the treatment of the individual, case management / care coordination, or recommendations for alternative treatments are not considered marketing and can be made without prior authorization. The ARRA appears to preserve these exceptions, so long as the provider is not being paid to make the communication. Moreover, even though the Act restricts payments for providing protected health information of an individual without consent, there are exceptions for treatment of the individual and for providing the individual with a copy of his or her medical record. In short, Microsoft believes that these new provisions will not damage patient-doctor communications. We will work with our business partners to analyze and comply with the new requirements.

Microsoft recognizes that there will be certain start-up costs associated with the new privacy requirements, as there are with most new regulations. In the long run, however, properly designed privacy protections can save money. Chief Information Officers at hospitals are already demanding technological tools that give them transparency into how health information is used and stored across their institutions, control over how that information is distributed, and secure methods of protecting

that information. These tools, which hospital CIOs need in order to improve quality and reduce costs, are the same technologies required to improve patient privacy. Effective privacy protections can foster the exchange and reuse of health data, which in turn can eliminate the need for unnecessary procedures, allow providers to make more accurate diagnoses, and contribute to important medical breakthroughs.

2. While I support a strong commitment to patient privacy, I am worried that some of the proposals under consideration would have unintended consequences for patients, physicians, and hospitals. Specifically, I am particularly concerned about a proposal that would prohibit the use or disclosure of protected health information for routine health care activities without individual consent. What are your thoughts on this type of proposal? Any thoughts on how a prior consent requirement would affect patient care, quality improvement and research?

Patients' health and well-being is the ultimate goal of the healthcare system, and Microsoft understands that privacy protections must be designed in a way that facilitates this outcome. The principles of transparency, control, and security can help create privacy safeguards that individuals both want and feel comfortable with. For example, two-thirds of Americans are willing to include their health data anonymously in a large database to help researchers.¹ When providers are transparent about the intended uses of the data—e.g., to help researchers—and when consumers can exercise control over how their data is shared—e.g., anonymously in a large database—better outcomes are achieved for everyone. Researchers have access to the data they need to make medical discoveries, and consumers benefit from research breakthroughs.

Under the ARRA, a covered entity cannot receive payment (either directly or indirectly) in exchange for providing protected health information without prior authorization. An exception is provided for, inter alia, the exchange of protected health information for public health activities, research, or treatment of the individual. Microsoft understands that the Department of Health and Human Services ("HHS") will be developing regulations to implement this provision, and we look forward to working with HHS and other healthcare participants to ensure that the new requirements do not hamper the delivery of effective patient care, quality assurance, and medical research.

3. Throughout all of your testimonies you all agreed that it is essential that there be privacy protections in place as we move nationally toward health IT. But, it seems that most of the ideas discussed were rather broad. Do you have any specific suggestions as to what privacy protections should be considered?

Microsoft appreciates the efforts made by Congress in examining and enacting the ARRA's privacy protections, and we are continuing to analyze the specific privacy provisions that were included in the legislation. Microsoft will work with HHS and others to ensure that regulations promulgated under the ARRA—including new regulations governing payment for the exchange of protected health information, breach notification, and the accounting requirement—bring the transparency, control, and security needed to drive changes in our healthcare system.

¹ Council for Excellence in Government et al., *The American Public on Healthcare: The Missing Perspective* (2008), <http://www.excelgov.org/Programs/ProgramDetail.cfm?ItemNumber=9404>.

4. Greater adoption of health IT has been recognized as enabling improved chronic disease management through better coordination of care. In order to coordinate care, providers need to be able to have access to patient data collected via health IT. For example, a provider could generate a list of all diabetic patients in a practice to ensure screening tests are up-to-date, prescriptions are filled, or to determine if any patients are overdue for a visit. What impact could privacy restrictions have on this and other care coordination functions?

Microsoft agrees that health IT can greatly benefit care coordination, and we are actively partnering with leading healthcare organizations to deliver novel improvements in chronic disease management. For example, our ongoing pilot project with the Cleveland Clinic is the first pilot in the country to follow multiple chronic diseases (specifically, diabetes, hypertension, and heart failure) in the clinical delivery setting using multiple at-home devices (e.g., glucometers, heart rate monitors, weight scales, and blood pressure monitors). Patients enrolled in the pilot upload device data to HealthVault using a home computer, and the Cleveland Clinic downloads the data into online charts accessible by treating physicians. Having data constantly monitored and shared in an efficient way can improve treatment decisions, quality of life, and management of acute care incidents.

Privacy protections can and should be designed to encourage these kinds of innovative uses of health IT. Appropriate privacy protections, based on the principles of transparency, control, and security, can actually improve care coordination functions. Once patients understand what their data will be used for, know who is looking at it and for what purpose, and are assured that their data is secure, they will be more inclined to share the health data that is needed for effective treatment and case management.

5. I have heard concerns expressed that by putting very narrow privacy constraints on the use of health information – like allowing specific information to be hidden and permitting medical treatment paid out-of-pocket to be kept secret – you encourage greater fraud and abuse, increase the incident of improper payments, and double-billing, among other things. What is your take or reaction to those concerns and what solutions, if any, would you propose?

As a general matter, Microsoft believes that effective privacy protections, including protections in the area of control, encourage patients to trust and participate in the healthcare system. However, Microsoft is concerned about a new provision in the ARRA under which individuals who pay out of pocket for a healthcare item or service can request that their data not be disclosed for payment purposes or not be used to conduct healthcare operations. A past study has shown that this kind of privacy-protective behavior can put individuals' health at risk.² Moreover, the restriction on the use of data in healthcare operations could negatively impact the availability of data for quality assurance and other vital healthcare functions. We believe that effective consumer education will be needed to help ensure that patients understand the consequences of hiding information and are willing to share health data with the providers who need that data in order to make sound medical decisions.

² California HealthCare Foundation, *National Consumer Health Privacy Survey 2005* (Nov. 2005), <http://www.chcf.org/topics/view.cfm?itemID=115694>.

III. Senator Hatch's Written Questions for Michael Stokes

1. Mr. Stokes, if I put my health data into HealthVault, what is Microsoft doing to protect the information it stores?

Microsoft recognizes that health data can be highly sensitive, and we have accordingly implemented strong measures to protect against the misuse of HealthVault data. One of our key principles is that individuals should control their own HealthVault data. Unless the individual gives explicit permission, data is not shared with third parties or others who seek to provide personalized ads or services.

In addition to the contractual protections we require from our business partners, Microsoft uses a wide array of technological and procedural protections to prevent hacking and other unauthorized intrusions. Our Security Development Lifecycle program 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 work closely with industry, consumer advocacy, and law enforcement partners to improve our coordinated response to security issues.

2. Mr. Stokes, you talk a lot about the importance of sharing data in your testimony. Why is it important for patients to share data? Can I share some, but not all, of my health data?

As my testimony indicates, it is important for patients to share data because the future of connected, patient-centric healthcare depends upon the exchange and reuse of health data. Right now, patients' health data is locked in silos, forcing physicians to either make treatment decisions based on incomplete data or else waste time and resources aggregating information. A health IT system that allows patients to connect their health data and share it securely from provider to provider would allow physicians to see patients' complete health history. More reliable data in turn enables providers to make better medical decisions, decrease wasteful spending, and increase the quality of care.

In consumer services such as HealthVault, individuals can choose to share some, none, or all of their health data. In fact, Microsoft provides many different tools to help individuals control the sharing of their data. In addition to controlling what data is shared, HealthVault users can control the who, the how, and the when: They can decide who else should have 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.

3. Mr. Houston, in your testimony you seemed to insinuate that de-identifying data would be too burdensome, time-intensive and costly. Are there no simple ways of removing the identifiable information? It would seem to me that because these are digital medical files the identifiable information could be easily removed using a computer. What are your thoughts? Mr. Stokes, do you have an opinion on this matter?

Microsoft understands that de-identifying data in a way that robustly prevents re-identification is a difficult technical challenge. However, we believe that de-identified data can be used in transparent, controlled, and secure ways that protect individuals' privacy, and we are investing in active research to develop new innovations in this area.

* * *

Microsoft recognizes that the protection of consumer privacy is a continuous journey, not a single destination. We can and will continue to develop and implement new privacy practices and protections for consumers as health IT becomes more widely used. At the same time, Microsoft acknowledges that technology is only a part of a comprehensive approach needed to drive real change in our healthcare system. Other critical components include education, leadership in healthcare organizations, and meaningful public policy. We look forward to partnering with all participants in the healthcare ecosystem to move toward dynamic, trusted, and consumer-driven healthcare.

Sincerely,

Michael Stokes
Principal Program Manager
Health Solutions Group
Microsoft Corporation