COMMENTS OF

MICROSOFT CORPORATION

In Response to the Federal Trade Commission's
Notice of Proposed Rulemaking and Request for Public Comment

On

Health Breach Notification Rulemaking, Project No. 911002

Section 13407 of Title XIII (HITECH Act) of the
American Recovery and Reinvestment Act of 2009

June 1, 2009

Microsoft welcomes the opportunity to provide comments on the Federal Trade Commission's request for public comments on Project No. 911002 with respect to health breach notification rulemaking.

Microsoft has strongly advocated for the adoption and implementation of policies that support and improve health care quality and reduce costs by promoting the increased adoption of health information technology (IT), resulting in faster and more reliable care in both populated and remote locations. At the same time, it is critical that consumers trust that their information is protected and that appropriate measures are taken where there is a data breach.

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 and security. 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 and security protections, we can realize the value of data sharing and thereby drive real change in our healthcare system.

Therefore, Microsoft is pleased to comment on the Commission's request for comments with respect to health breach notification under Section 13407 of Title XIII (HITECH Act) of the American Recovery and Reinvestment Act of 2009.

Specifically, Microsoft would like to comment on six elements of the proposed rule:

1. Notification to Pseudo-anonymous Users

Many online health IT-related services, including Microsoft's HealthVault, do not require users to provide full contact information to sign up for an account. Users may provide minimal contact information or they may provide fictitious names or incorrect addresses, telephone numbers, and other contact information. Microsoft has consulted with leading

privacy advocates who believe this is an option that users should have in order to minimize the amount of identifiable personal information required to open an account.

The proposed rule could be interpreted to require that if a service must notify users of a breach under Section 13407, it would be required to request additional address information from such pseudo-anonymous users in order to provide the statutorily required breach notification in written, non-electronic form. While the proposed rule allows services to obtain explicit prominent consent for email notification, we recommend that accounts created prior to the effective date be allowed to use the information users provided as the preferred contact method. Otherwise services will be required to contact users to obtain additional personal information in the form of a physical address or telephone number that they previously chose not to share with the service. If existing users do not reply to this request, it is ambiguous how the service should comply with the rule.

We believe that Section 13407 should allow notification in the manner and to the location a user has chosen to communicate with the service. A user who has chosen not to provide complete or correct address information permitting postal mailing, but has provided an email address, should be presumed to have expressed a preference to receive email notices, including for the purposes of Section 13407. A service should not be required to request, or a consumer asked to provide where they do not want to, additional contact information in the event of a breach.

2. Scope of Personal Health Record (PHR) Definition

We urge the Commission to collaborate with the Department of Health and Human Services (HHS) to clarify the definition of a "personal health record," which is important to the interpretation of HITECH generally and to the recommendations that the Commission and HHS will provide on the application of privacy and security requirements to non-HIPAA covered entities under Section 13424(b) of HITECH. We share the concerns raised by others, including the Markle Foundation Connecting for Health Initiative, that the current definition, "an electronic record of PHR identifiable health information . . . on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or for the individual," could be interpreted to cover services whose intended or primary use is not healthcare related. For example, a user could store health information in a Web-based email system such as Hotmail, or a social networking site such as Facebook.

We do not believe that Congress intended such services to be subject to the same level of regulation as dedicated PHRs. In many cases, service providers are not able to know or control what information users maintain on their services. Even if users are prohibited from storing health information by the service's terms of use, service

providers are largely unable to verify whether users comply. One suggestion to clarify this definition would be to include "intended use " into the definition in a manner similar to FDA regulations. This would result in a definition of "an electronic record whose intended use is a PHR of identifiable health information . . . on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or for the individual,"

We urge the Commission to continue close cross-agency coordination with HHS to ensure consistency across breach of health information notification rules. As the health industry quickly evolves and transforms, technology continues to evolve and new solutions are found, the lines between different types of entities could become blurred and some entities may evolve into different classifications. Consistency across agencies promotes and enables best practices for breach notifications irrespective of which entity classification is regulated by a specific agency.

3. Definitions of PHR Related Entity, Third Party Service Provider, and Vendor of Personal Health Record

The proposed definitions of the terms "PHR related entity," "third party service provider," and "vendor of personal health records" each refer simply to "an entity" that meets the definition's criteria. It is not clear how the definitions apply to entities that have many operations, only some of which meet a definition's criteria. We recommend that the Commission clarify the scope of these definitions using a concept similar to the "hybrid entity" rules under the HIPAA Privacy and Security Rules. See 45 C.F.R. §§ 164.103 and 164.105(a) in order to optimize the economic impact of these rules

In addition, the terms "PHR related entity" and "third party service provider" should clarify what happens when an entity is unaware that it is dealing with a PHR vendor. For example, a cloud service provider may offer computing power and storage without knowing whether customers use them to maintain or offer PHRs. We recommend that PHR vendors be required to inform PHR related entities and third party service providers of their status.

4. Use of Telephone Number in Notice to Media or Web Posting

The Commission's proposed Section 318.5(a)(4)(ii) requires that "notice in media or web posting shall include a toll-free phone number where an individual can learn whether or not the individual's unsecured PHR identifiable health information may be included in the breach." In many cases, it will be difficult for a PHR vendor or other entity subject to this requirement to authenticate a caller over the telephone. By contrast, where a consumer already has an online account with the PHR vendor or other entity, the consumer may more naturally and more securely log into his or her account to learn about the breach and whether it affected the consumer's data. We

recommend that an entity be permitted to offer a method other than a toll-free number for consumers to use to learn about a breach if the entity believes in good faith that the other method is more appropriate.

5. Notice to Commission; When Breaches are Treated as Discovered

HITECH Section 13402(e)(3) requires that HIPAA covered entities give notice to the Secretary of HHS of security breaches and that "[i]f the breach was with respect to 500 or more individuals th[e]n such notice must be provided immediately." Section 13407(a)(2) similarly requires PHR vendors and other entities subject to the notice requirements of Section 13407 to notify the Commission. Although Section 13407 does not itself define a timeframe, it incorporates the timeliness requirements of Section 13402.

The Commission's proposed new Section 318.5(c) interprets the timeliness requirements of HITECH to require giving notice to the Commission "as soon as possible and in no case later than five business days following the date of discovery of the breach."

The Commission also defines a breach as discovered when it is known to any "employee, officer, or other agent" of the entity experiencing the breach (other than the individual committing the breach). The Commission's definition follows closely the statutory definition in HITECH Section 13402(c), which is incorporated into Section 13407.

While five days may in some cases be sufficient time for an entity to provide notice, it may not always be sufficient time. Since the knowledge of almost all of the entity's employees, officers, and other agents is imputed to the entity, it will take some time for the person discovering the breach to notify the entity's compliance department. And, as the Commission recognizes in footnote 19 of its section-by-section analysis of the proposed rule, important facts such as the number of consumers affected or the extent of the information breached may not be known at the end of the five days. Since the number of consumers affected is the threshold for the notice requirement, a five-day deadline may result in needless notifications to the Commission about breaches that likely affect fewer than 500 individuals when the entity is unable to prove that definitively before the deadline.

We suggest that the notice requirement in the final regulation use the statutory language of "must be provided immediately." We recommend that the Commission adopt a flexible approach to interpreting that statutory language. In particular, when an entity does not reasonably believe that a breach affects more than 500 individuals, it should not be required to notify the Commission immediately (understanding that it must

notify the Commission as soon as its investigations uncover that the breach does affect more than 500 individuals).

6. Unsecured Identifiable Health Information

As with many state laws and proposals for a federal data breach notification legislation, Microsoft supports including an exception to the notification requirement where measures are used to render data unusable, unreadable, or indecipherable to any party that gains unauthorized access and are widely accepted as an effective industry practice or an industry standard. As the FTC and HHS craft guidance on the definition of “unsecured”, any recommendations should remain technology neutral. Security information technology evolves and “locking-in” a specific method may result in stifling the development and use of other better technologies to protect sensitive data.

Conclusion

Data breach notification can play an important role in ensuring continuing consumer trust of health care technologies. Microsoft also appreciates that technology is being created and evolving very quickly – responding to the need for better access, quality and outcomes for consumers and health providers. This environment means that providing guidance and rules that consider what technology exists, and the role different technologies play, is increasingly challenging. Our comments reflect that environment.