Public Testimony

To: Office of the National Coordinator, Policy Committee, Department of Health and Human Services

CC: Wayne Gattinella, Craig Froude, Bob Marotta, Doug Wamsley, Charlie Mele, Tony Vuolo, Matt Kaminer

From: Philip Marshall MD, MPH VP of Product Strategy, WebMD Health

Date: September 18, 2009

Topic: **Data Storage and Exchange, Aggregate Data, De-Identification and Re-Identification**

Distinguished members of the Committee,

It is my pleasure to represent WebMD on today's panel to discuss data storage and exchange, aggregate data, de-identification and re-identification.

Overview of WebMD and the Secure Storage and Exchange of Health Information

WebMD has three divisions, including the WebMD Health Network which is the leading provider of health information to consumers with approximately 60 million unique visitors each month, Medscape which is the leading provider of health information to healthcare professionals and the leading provider of Continuing Medical Education programs online, and WebMD Health Services which is the leading provider of Health and Benefit Management solutions to large employers, health plans, and government entities. Within this last division, we make available a Personal Health Record to millions of users. We have provided personal data storage and management services for more than 10 years, and secure data exchange with professional data sources for more than 5 years.

Our testimony pertains to the data storage, exchange, aggregation and de-identification that occur in support of this last division and in its delivery of a Personal Health Record service.

Secure Consumer Data Storage and Exchange with the WebMD Personal Health Record

Personal Health Record services at WebMD are provided in conjunction with our payer and employer customers. WebMD has HIPAA Business Associate agreements in place with each of the plan or plan sponsor customers for whom we provide PHRs that integrate professional data, and data use agreements are in place with their data providers such as Third Party Administrators, Data Warehouses and Reference Laboratories.

The purpose behind data exchange with the Personal Health Record is to allow our consumer end-users to gather, store, manage and share their data, helping them and their care providers

make more informed decisions. We believe that the Personal Health Record can help achieve the objectives shared by key participating stakeholders – consumers, providers, employers and payers – to provide a greater continuity of care in order to improve quality and lower costs. Serving as a BA to Covered Entities, WebMD supports and adheres to the HIPAA Privacy and Security Rules.

WebMD believes in giving our consumer users control over how their data is managed and shared. We do not share identifiable health information with employers, although consumers can choose whether or not to share their information with health plans and the health plan services that those plans provide such as disease management services. Our guiding philosophy of consumer control and choice is in line with the Markle Foundation's Common Framework and their Consumer Principles for Health Data Exchange, which WebMD helped to author.

WebMD provides data security on multiple levels, including physical, network, system, and application security. WebMD stores data securely on database systems which are mirrored on the east and west coasts. All identifying data is encrypted on the database servers, with individual-specific encryption keys held separately from the database servers. Our de-identification process complies with the Safe Harbor methodology to remove the 18 data types that could be used for patient identification. De-identified data is stored in WebMD's secure data warehouse for purposes of aggregate reporting internally and aggregate reporting to our clients. These reports include aggregate usage data and aggregate health risk analysis reports. In addition to using de-identified data, our reporting tools enforce a limitation of cell size or drill-down for any clinical or health-related data to a 50 individual minimum, helping to eliminate any chances of identity inference.

For technical interoperability, WebMD supports the CCR and CCD standards for document exchange. We have implemented HL7 standards for lab test result data exchange, as well as a variety of file formats for administrative (claims) data exchange. File transfers have generally been PGP-encrypted batch exchanges, although WebMD does conduct real-time secure exchange of data with some partners. The CCR standard is simpler to work with and implement than CCD, and we will likely use the CCR standard with data partners where the CCD standard is not required. However, WebMD has implemented support for the CCD standard and will be exchanging data with clinical systems using that standard, along with using other aspects of the HITSP C32 construct.

For semantic interoperability, WebMD has long supported SNOMED CT, LOINC and the common billing vocabularies, and is implementing RxNorm for medication data interoperability. WebMD's own Thesaurus infrastructure uses these vocabularies in a variety of ways, including the mapping to consumer understandable terms where necessary.

Feedback on Recent Policy Committee Discussions and Publications

WebMD applauds the Committee for the publication of Meaningful Use objectives and measures that support patient engagement and the patient's ability to receive copies of their information. We also believe that the published findings and recommendations of the Health

Information Exchange workgroup are consistent with our point of view. WebMD is pleased to provide the following feedback regarding recent discussions and publications:

1. The 2011 Meaningful Use objectives and measures specify that patients should be given access to their information, and by 2013 be given an electronic copy. The 2011 objectives and measures are inconsistent with ARRA in that ARRA specifies that the individual shall have a right to obtain from the covered entity a copy of their information in an electronic format and, if the individual chooses, to direct the covered entity to transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific. WebMD believes that the ability to get a copy of information is essential to ensuring that patients and their treating care providers have access to information from across the continuum of care, and we request that the timing of gaining a copy, vs. simple access, be reconsidered.
2. WebMD agrees with the Health Information Exchange workgroup in prioritizing transport/communication standards and container/envelope standards as initial steps in achieving greater data fluidity.
3. WebMD believes that there are specific barriers to consumer-centric data exchange that the Policy Committee should address. In particular, the inability for consumers to access their lab test results unless released by the ordering provider is a significant barrier to consumer engagement and consumer-driven health improvement. If health plans through their provider contracts can have legal access to this information, and if HIPAA and now HITECH enable consumers to get their own information from covered entities, then consumers should be able to get their own data directly from the labs as well.
4. WebMD believes that the complexities of semantic interoperability will be critical to address. The clinical operations workgroup has recognized vocabulary standards as critically important, and WebMD is pleased to support the use of SNOMED CT, RxNorm, and LOINC, among other standard vocabularies. The semantic consistency of data is not only important for presentation within consumer applications, but eventually also for the aggregation and analysis of de-identified data as well.

Finally, WebMD participates on the CCHIT Personal Health Workgroup, and we fully support the efforts to define certification criteria for PHRs. Such criteria, however, must be consistent with the data exchange required for proving Meaningful Use and consideration should be made for how the CCHIT PHR certification could complement the exchange required under Meaningful Use. WebMD's recommendation is that Personal Health Records have a certification process that certify that PHR systems have the appropriate privacy, security and technical capabilities to support other systems in achieving the Patient Engagement component of Meaningful Use, whether that certification be conducted through CCHIT or elsewhere.