



Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

February 18, 2011

Re: IMS Health Comments on “Protecting Consumer Privacy in an Era of Rapid Change”

Dear Sir or Madam:

IMS Health respectfully submits these comments related to the Preliminary Federal Trade Commission (FTC) Staff Report entitled, “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers” (hereafter referred to as “the proposed Framework”).

We appreciate this opportunity to comment and offer:

- (1) Background: IMS Health and our history of data stewardship, and
- (2) Discussion: Comments regarding various aspects of the proposed Framework, including laudable ideas, areas of concern and other thoughts to be considered.


BACKGROUND:

IMS Health is the world’s leading provider of health information and analysis to healthcare stakeholders. With a presence in more than 100 countries and over 55 years of experience, IMS Health applies leading-edge technologies to transform billions of healthcare transactions collected from thousands of sources into data sets, files and extracts that provide strategic insights vital to effective management of healthcare and healthcare systems. Interpreted and analyzed by IMS Health experts, the data and analyses are an unmatched source of trends and perspectives about healthcare for clients that include healthcare companies, governments, payers and academic researchers.

IMS Data Stewardship:

As a global leader in information solutions, IMS is an international leader in health information stewardship — including privacy and data protection. We firmly believe that patient health information, used wisely and responsibly, advances worldwide medicine and results in real value for healthcare communities. We believe just as firmly that this information, by its nature, can be highly sensitive to an individual and that individual privacy must be preserved and protected.

As a company, we are patient privacy and data protection advocates — and since our founding, IMS Health has pioneered commercial practices to de-identify individual patients and sensitive data. This is a key component of our core competency in privacy. IMS Health relies on a combination of resources, policies and practices to ensure the



leadership necessary to manage this information in a manner that balances a range of societal values, including the promotion of improved healthcare and individual privacy.

DISCUSSION:

IMS Health supports the Commission's interest in consumer protection as it relates to privacy and security. Further, we appreciate the outreach the Commission has shown in the form of privacy roundtables to learn more about existing privacy and security concerns and existing privacy and security successes and best practices. We encourage the Commission to continue this dialog with stakeholders, coupled with a review of all existing state and federal laws, rules and regulations related to privacy and security, to enable the best possible approach to privacy and security going forward.

THE PROPOSED FRAMEWORK'S SCOPE AND INTERACTION WITH EXISTING REGULATORY FRAMEWORKS

Healthcare Industry's Regulatory Scheme

The principles supporting the proposed Framework (Privacy by Design, Simplified Choice, Greater Transparency) are laudable principles that underlie other existing privacy and security frameworks.

For example, in the healthcare sector, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act support these concepts in the form of legal obligations.

The existing HIPAA/HITECH framework establishes privacy and security requirements for Covered Entities and Business Associates (as defined by HIPAA) that are similar to those proposed by the Commission in its Fair Information Practice Principles (FIPPs) of Notice, Choice, Access, Security and Enforcement.

Specifically, with respect to HIPAA and HITECH:

- 1) A basic tenets is that of using and disclosing only the "minimum necessary" protected health information;
- 2) The "Notice of Privacy Practices" offers transparency in the form of a description of how protected health information is used and disclosed;
- 3) Patient Rights: Access, Accounting, Amendment, Confidential Communications, Restriction ;
- 4) Security when handling protected health information in the form of administrative, technical and physical safeguards;
- 5) Enforcement is vested in the Department of Health and Human Services (HHS)/Office for Civil Rights (OCR).

Moreover, the members of the healthcare industry understand that consumer trust is an important component of their business models. Protecting the confidential information entrusted to them is a primary concern, and most have developed robust policies, procedures and technical solutions that may go beyond legal requirements and consider public policy, self-regulation and best practices. These organizations realize they are accountable to the individuals whose data has been entrusted to them, they take responsibility for the data they safeguard, and they are answerable for their data handling practices.



Recommendation #1

The extensive, detailed and complex HIPAA/HITECH framework has requirements that go beyond those suggested by the proposed Framework, and we see no need for the Commission to impose additional, and potentially inconsistent, privacy and security practices on the healthcare industry. We recommend that the healthcare sector, which is already subject to regulation, be excluded from the Commission's final report, and that the report should focus on those economic sectors not already subject to privacy and security regulations.

Framework's Feasibility for Data that can be Reasonably Linked

We appreciate the Commission's specific request for comment regarding the practicality of applying the proposed Framework to data that can be "reasonably linked to a specific consumer, computer or other device."

While we understand the Commission's concerns around changes to the traditional distinction between personally-identifiable information (PII) and non-PII, we also believe that any abilities to re-identify consumers from anonymous data can be appropriately managed through responsible data handling processes and existing consumer protection remedies.

As already discussed, the proposed Framework is remarkably similar to the HIPAA/HITECH framework. One distinction is that HIPAA/HITECH exempts "de-identified" data¹ from many front-end requirements of its framework that apply to health information that is individually identifiable and known as protected health information (PHI). However, on the back end, a re-identification of de-identified data could lead to enforcement actions (potentially in the forms of civil monetary penalties, sanctions or criminal penalties as determined by the regulatory authority, OCR).


This legal and regulatory concern is certainly not taken lightly by those who routinely handle de-identified information. Further, the overarching concerns regarding consumer trust in the safe handling of their healthcare information drives and guides businesses to treat de-identified information with the utmost care and respect throughout its lifecycle.

Some aspects of the proposed Framework's privacy by design concept can be utilized by those handling non-PII data. For example, robust technical, physical and administrative security safeguards should be employed when handling not only PII, but also information that might reasonably be linkable.

Applying the proposed Framework's choice and notice provisions is much more difficult when dealing with non-PII, however.

The proposed Framework's "commonly accepted practices" are very similar to the "treatment, payment and healthcare operations" functions exempted from the patient authorization requirement for PHI under HIPAA. This implied consent concept is extremely important in ensuring that access to critical data is not impeded and that consumers and businesses continue to smoothly undertake their routine business transactions.

¹Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. 45 CFR 164.514.



For those non-routine situations, obtaining consent for the use or disclosure of PII theoretically sounds like a good idea. However, in practice this is often not feasible. Consent cannot always be informed, especially given the complexity of some data collection and use. If an individual cannot make a truly informed and knowledgeable decision, the consent is not meaningful and merely becomes an exercise in checking off the box to say consent was obtained.

This is even more troublesome when we consider applying a consent requirement to data that is non-PII. We cannot obtain real-time consent for non-PII, because, by definition, we do not know who the individual is – absent re-identification, the very situation we are trying to avoid. If a person gives consent at the time of data capture and the data is later rendered anonymous or de-identified, he or she cannot modify his/her grant of consent unless he or she can be tracked through data re-identification. Revoking consent is problematic, and granting consent for new uses of the data is also a problem without re-identification of the individual.

It is also difficult to provide notice to persons concerning the use of their non-PII for many of the same reasons. Without re-identification, changes in privacy notices cannot be given to individuals – and it's nearly impossible to properly anticipate any and all potential uses and disclosures of non-PII at the time of data collection. Further, it's unrealistic to expect that there will not be changes in privacy notices from time to time, whether due to changing legal requirements, changing privacy or security practices, sales or mergers of the business, etc.

Recommendation #2

While we strongly believe that non-PII should be adequately safeguarded from risks of re-identification or misuse, we do not believe that including “reasonably linkable” information in the scope of the proposed Framework is helpful. There does not appear to be a significant privacy benefit from so doing, and the practical application is fraught with significant problems. Rather, we propose that reliance upon existing frameworks (e.g., in the case of health information, reliance upon HIPAA/HITECH and OCR oversight) and consumer protection remedies available to the Commission be used to ensure this data is protected.

EDUCATION

We wholeheartedly agree with the need for greater consumer education to increase consumer awareness and understanding of overall data collection and use practices and their privacy implications, and the benefits that may be obtained from the use of the data as well.

In a research survey of American voters undertaken by IMS Health last year, one key finding was that a majority of voters expressed a willingness to share their anonymous healthcare information for research – but that a significant number felt concern about the privacy of their medical information. This, coupled with other key findings around a lack of knowledge of healthcare terminology and a distrust of key leadership, told us that education is crucial to moving not only healthcare, but also privacy, forward. Unless consumers truly understand the intricacies of how their PII or anonymous information is being used and how it might benefit themselves and others, their decisions are not informed and their concerns may or may not be realistic.



Recommendation #3

In addition to having businesses, consumer groups, academics and non-profits perform educational outreach campaigns, we respectfully request that the Commission and other branches of state and federal government join in this effort. Some of the most memorable and effective consumer awareness campaigns have occurred because of the leadership of the Commission (e.g., the FTC ID theft awareness campaign, among others).

Thank you for the opportunity to comment on the proposed Framework. Additionally, if you desire to discuss our comments or suggestions further or if you have any questions, please feel free to contact me.

Sincerely,

Kimberly S. Gray, Esq., CIPP
Chief Privacy Officer, Global
IMS Health
KGray@us.imshealth.com