surescripts
The Nation's E-Prescription Network

February 18, 2011

The Honorable Jon Leibowitz
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: Federal Trade Commission, A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers -- File No. P095416

Dear Chairman Leibowitz:

Guided by the principles of privacy, security, neutrality, choice, transparency, collaboration and quality, Surescripts operates the nation's largest health information network. The Surescripts network supports the most comprehensive infrastructure of healthcare organizations nationwide. Pharmacies, payers, pharmacy benefit managers (PBMs) physicians, hospitals, health information exchanges (HIEs) and health technology firms rely on Surescripts to more easily and securely share health information. By providing that information during emergencies and routine care, Surescripts is committed to saving lives, improving efficiency, and reducing the cost of healthcare for all. You and your staff can learn more about Surescripts by visiting our web site, which is located at www.surescripts.com.

As creators of the first and only nationwide means of electronically sharing health information, Surescripts feels a responsibility to state clearly and plainly who we are and what we believe. We do this by publicly stating our principles. Surescripts' principles both outline our philosophy as an organization and enable connections between the nation's health care participants.

1. **Security and Privacy.** We constantly review and update all procedures and technology to guarantee the integrity of our system and to ensure everyone's privacy is protected. More information can be found at http://surescripts.com/about-us/commitment-to-privacy.aspx.

2. **Neutrality.** Surescripts implements and consistently applies objective standards for certification and implementation of technology systems that promote an open, neutral network and interoperability.

3. **Choice.** Surescripts' network is designed to support patient choice of pharmacy and prescriber choice of drug therapy. Commercial messaging is not allowed on the network. In addition, our choice to focus on the certification of e-prescribing and EHR software — and not its development or sale — helps ensure a wide choice of options for providers.

4. **Transparency.** Our policies are made public to current and potential network participants through extensive participation in government and industry workgroups and through Surescripts own workshops and documentation.

5. **Collaboration.** Surescripts works throughout the healthcare community to develop educational programs, quality initiatives, and certification standards, and to promote dialogue to support the future growth of e-prescribing and health information exchange.

6. **Quality.** Making health information electronic is not enough – it must be accurate. Through our quality program, we measure, analyze and take action to ensure the accuracy and reliability of prescription information, from the time the prescription is prepared to the time it is dispensed.

Given Surescripts' central role in health information technology (HIT) in the U.S. today, we were keenly interested in the concepts, issues, and recommendations raised by the referenced Federal Trade Commission (FTC) proposed framework. We are pleased to offer our following comments. Surescripts applauds the FTC's efforts to examine and address consumer concerns regarding information privacy. We recognize that this is especially important in the health care arena and has become a primary area of focus for a wide range of actors including numerous federal and state regulators. We believe that our underlying principles support the proposed framework's overarching intent to protect consumer privacy.

General Comments

The world of HIT has greatly expanded in recent years and we, as a health information network, continually strive to address privacy and security concerns that are, in large part, governed under a complex set of privacy laws—from the Health Insurance Portability and Accountability Act (HIPAA) as amended by the Health Information technology for Economic and Clinical Health (HITECH) to state privacy laws and consent models. Additionally, a number of policy committees and workgroups are also examining and making recommendations regarding privacy and security issues related to HIT.

The proposed framework is a positive effort by the FTC to address consumer privacy concerns, focusing primarily on online usages and practices that have remained largely unregulated due (in part) to ongoing advances in technologies. However, a number of efforts are currently being undertaken or already exist in the healthcare environment addressing many of the same concerns the proposed framework focuses on (*e.g.*, the HIPAA Privacy and Security Rules, as modified by HITECH). HIPAA covered entities and business associates are required to incorporate substantive privacy and security requirements within their organizations when dealing with third

parties. Additionally, such entities may only use and disclose protected health information for limited, enumerated purposes in accordance with the Privacy Rule provisions and consent and authorization are also addressed. HITECH recently extended many of the HIPAA provisions to cover business associates and specifically categorized new entity types as business associates, all directly accountable for their entities' actions under the law.

Outside of the HIPAA context, the Office of the National Coordinator, through its HIT Privacy Committee is also examining privacy and security issues in the HIT arena. States also routinely regulate how and when consent for the use and disclosure of health information is permissible and under what circumstances.

Given the complex web of existing laws, regulations, best practices, and the like with respect to health information practices, we urge the FTC to narrow the scope of the framework to exclude such in order to prevent additional duplicate and/or divergent frameworks. Such an exclusion would permit currently-regulated entities to continue building upon their extensive efforts to comply with existing applicable law. Alternatively, we urge the FTC to coordinate its efforts with other privacy efforts to ensure consistent health information privacy policy development and implementation.

Specific Comments

I. Scope

Surescripts Comments: Surescripts believes that it would not be appropriate for an umbrella framework to cover all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. As noted above in our general comments, we are concerned that adding another layer to the existing regulatory web could lead to increased disconnects and conflicting obligations than already exist.

Are there practical considerations that support excluding certain types of companies or businesses form the framework—for example, businesses that collect, maintain, use a limited amount of non-sensitive consumer data?

Surescripts Comments: We urge the FTC to exclude companies subject to other frameworks (such as HIPAA) addressing the issues be excluded to the extent the activities are covered in duplicate. Alternatively, we urge the FTC to coordinate terminology and requirements under the proposed framework with other laws and regulations (including both federal and state laws) governing entities involved with protected health information.

Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device"?

Surescripts Comments: See comments above.

II. Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

Surescripts Comments: As a general concept, Surescripts applauds and understands the importance of the concept of privacy by design and currently implements such in our operations. For example, we have established policies and procedures in accordance with HIPAA that are designed to promote consumer privacy. We also ensure that our data is protected and used in accordance with our notice of privacy practices. Data is encrypted is currently being addressed under the HITECH mandates and HIPAA breach notification proposed rulemaking processes (which interim rule recommended the National Institute of Standards and Technology (NIST) Special Publication 800-11 for data at rest and the Federal information Processing Standards (FIPS) 140-2 for data in motion, among other sources. Therefore, we urge the FTC to coordinate the proposed framework with existing industry guidance.

Incorporate substantive privacy protections
Should the concept of "specific business purpose" or "need" be defined further and, if so, how?

Surescripts Comments: Surescripts does not believe that the concepts of "specific business purpose" or "need" should be further defined and may be more appropriately addressed by commercial entities providing greater transparency with respect to their data practices.

Is there a way to prescribe a reasonable retention period?

Surescripts Comments: Surescripts recommends that the FTC coordinate any such efforts with existing law. Additionally, we urge the FTC to adopt a flexible approach so impacted entities may appropriately asses risk management of such retention against the business needs, consumer needs and legal requirements. Incorporating such flexibility will accommodate differing business models, data uses, and consumer concerns. For example, it may be beneficial for a certain data to be retained for longer terms than other types (*e.g.*, the length of time that medication history is relevant may be longer than other types of information such as information needed to complete a single transaction).

Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that retention periods for such data can be quite short?

Surescripts Comments: Yes, we believe that retention periods may be largely dependent upon the type of data at issue. Please see our comments above for additional discussion.

Maintain comprehensive data management procedures throughout the life cycle of their products and services.

Surescripts Comments: Please see our general comments above regarding existing data management procedures under Section II above. Additionally, we note that a number of data management frameworks currently exist (*e.g.*, International Standards Organization (ISO) Guides 27001, *Information Security Management System*, and 27002, the code of practice for information security management, NIST publications, and Information Systems Audit and Control Association (ISACA) publications).

III. Companies should simplify consumer choice.

Surescripts Comments: Please see our general comments above regarding HIPAA applicability. HIPAA has a framework for consent and authorizations with respect to certain healthcare transactions. For example, consent for payment, treatment, and health care operations (commonly referred to as PTO) is not required. Additionally, to address situations that are not covered by HIPAA, the HIT Policy Committee's Tiger Team has made recommendations regarding consent for electronic exchange of patient identifiable health information among known entities. As such, we strongly urge FTC to ensure that its efforts do not conflict with or unnecessarily undermine efforts previously taken by commercial entities to comply with such.

Commonly accepted practices

Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?

Surescripts Comments: See comments above in Section III.

How should the proposed framework handle the practice of data "enhancement," whereby a company obtains data about its customers from other sources, both online and offline, to enrich its databases? Should companies provide choice about this practice?

Surescripts Comments: In the context of healthcare, it is common for companies such as Surescripts to create directories. In some cases, directories are compiled from information received from prescribers and may need to be updated and/or supplemented from information received from another source to maintain the directory. Having to provide choice regarding such directories could create undue hardship and delay and impact the quality of data available for use for business operations and the advancement of health information exchange in a protected manner.

Practices that require meaningful choice
General

Surescripts Comments: Please see our general comments above.

How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts?

Surescripts Comments: Many states and federal regulations (HIPAA, the Substance Abuse Confidentiality Regulations, etc.) currently address "sensitive" information and how consent and uses and disclosures of such information should be handled. We urge FTC to coordinate efforts in this arena to avoid duplicative and confusing requirements.

Companies should increase the transparency of their data practices.

Surescripts Comments: As part of our core principles discussed above herein, Surescripts believes its practices should be transparent to the public and our practices are made known in a variety of forums, from our notice of privacy practices to governmental, industry, and customer workshops.

Improved privacy notices

What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

Surescripts Comments: As noted in the FTC's discussion, data practices vary greatly across industries. Reconciling common language across the existing web of defined legal terms could be time-consuming and complicated with a less-than-desired outcome.

Reasonable access to consumer data

Surescripts Comments: HIPAA similarly speaks to individual access to protected health information as a subset of consumer access addressed in the proposed framework. For example, the Privacy Rule permits individuals to access their health information from a covered entity. All covered entities must enter contractual relationship to require its business associates and downstream subcontractors to provide the covered entity with non-routine or improper uses and disclosures of protected health information. Additionally, business associates must also provide protected health information in its possession to a covered entity to allow a covered entity to comply with its legal responsibilities to provide authorized individuals accountings of disclosures, and amendments or access to such protected health information. More recently, HITECH has also mandated accountings of routine disclosures of health information in certain circumstances and attendant regulations are anticipated in the near future.

Should companies be able to charge a reasonable cost for certain types of access?

Surescripts Comments: We agree that companies subject to access requirements be able to recoup the cost associated with such access, including the labor costs to retrieve and present such data.

Should access to data differ for consumer-facing and non-consumer-facing entities?

Surescripts Comments: Surescripts believes that access to data should be different for non-consumer entities that have a direct obligation to provide such information to consumer-facing entities, as discussed above.

We thank you for the opportunity to comment. If you have any questions, please feel free to contact either of us at: 703.921.2179 or Paul.Uhrig@Surescripts.com; 703.921.2119 or Kelly.Broder@Surescripts.com.

Sincerely,

/s/ Paul Uhrig

Paul L. Uhrig
EVP, Chief Administrative & Legal Officer; Chief Privacy Officer

/s/ Kelly Broder

Kelly L. Broder
Associate General Counsel