February 18, 2011

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

Dear Chairman Leibowitz:

With an increasingly networked environment in which consumers interact with applications and services that collect personal information around the clock, it is imperative to have strong policies and practices in place that will earn consumer trust. We support the Federal Trade Commission's (FTC) call for industry to adhere to a comprehensive framework for consumer privacy and data protection that is based on Fair Information Practices (FIPs).

Markle Connecting for Health, a public-private collaborative of more than 100 organizations across the spectrum of health care and information technology (IT), appreciates the opportunity to comment on the FTC's preliminary staff report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*.[1] This letter is nearly identical to comments we are submitting to the US Department of Commerce regarding that agency's recently released green paper, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.[2] Our comments build on a decade of collaborative work, including the Markle Connecting for Health Common Framework for Networked Personal Health Information, which details specific policies and practices for organizations that collect, share, and store health information on behalf of consumers.[3] This

---

1 Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers; Preliminary Staff Report." 2010. Accessed on Web January 17, 2011: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

2 Department of Commerce Internet Policy Task Force. "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." 2010. Accessed on the Web January 10, 2011: http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

3 Markle Foundation. *Markle Connecting for Health Common Framework for Networked Personal Health Information*. June 2008. Accessed on Web January 17, 2011: http://www.markle.org/health/markle-common-framework/connecting-consumers.

Markle Common Framework, endorsed by fifty-seven organizations[4]—representing consumers, patients, technology companies, providers, insurers, clearinghouses and privacy experts—was developed specifically by applying a set of principles based on FIPs to the emerging environment of new personal health information applications and services largely unregulated by the Health Insurance Portability and Accountability Act (HIPAA), and translating them into specific policies and practices that can be used to establish a consistent framework for trust.

Although both the FTC staff report and the Department of Commerce green paper pertain to commercial uses of consumer information generally, our comments focus primarily on personal health information—which is being collected, analyzed, and shared in a widely increasing variety of contexts.

Our comments fall into three primary areas. First, we commend both the FTC and the Department of Commerce for their emphasis on a full complement of FIPs. Second, we urge coordination of federal policies, rules, regulations, and jurisdictions, specifically in the area of personal health information. Third, we point to a need, if we are to fulfill consumer expectations, for an even more forward-looking and consistent cross-sectoral approach to privacy and security protections. As the use of the Internet continues to evolve to create new information and service intermediaries, consumers will inevitably expect protections to be in place across the spectrum of organizations that hold their personal health information, regardless of sector-specific boundaries. Health profiles on individuals are compiled by a wide range of organizations both inside of health care (e.g., providers, insurers, pharmacies, and clearinghouses) and outside of health care (e.g., Internet sites, personal health record services, mobile apps, marketers, advertisers, and search engines). Focusing on consistent protections for consumers will have the dual effect of enhancing market certainty for business and fostering an environment of trust in which consumers can safely engage.

Federal policymakers have good reason to consider the privacy of health information. It is a significant concern for the American public and doctors who serve them, according to recent surveys commissioned by the Markle Foundation. More than 80 percent of the public and doctors surveyed consider privacy safeguards an important requirement to ensure that health IT incentives under the Health Information Technology for Economic and Clinical Health (HITECH) Act will be well spent. Seventy percent to 80 percent majorities of both the public

---

4 Markle Foundation. *Common Framework for Networked Personal Health Information: Statement of Support*. June 2008. Accessed on Web January 19, 2011: http://www.connectingforhealth.org/resources/CCEndorser.pdf.

and doctors surveyed also support privacy-protective practices such as letting people see who has accessed their records, notifying people affected by information breaches, and giving people mechanisms to exercise choice and correct information.[5]

Background: Market Evolution Is Blurring Lines

We agree with the conclusions in both the FTC and Department of Commerce reports that the privacy ecology has transformed dramatically throughout the years. Countless data-collecting applications and services now have very broad market penetration and high levels of persistence in generating electronic profiles of individuals. It is encouraging that both reports recognize that there are shortfalls in both the current policy framework and in today's business practices to adequately and consistently protect consumer information and afford choice. Both agencies embrace the importance of FIPs as a framework for evolving a set of more comprehensive protections going forward.

The large, diffuse health sector is particularly complex in its various collections, uses, and sharing of personal information. Evolving business relationships and data flows have blurred distinctions about services covered by HIPAA. Personal health information services may be considered HIPAA Covered Entities in one context, yet Non-Covered Entities in another context.[6] HITECH broadened to some extent the circumstances under which traditionally Non-Covered Entities must comply with the HIPAA privacy and security rules, but gray areas remain. Most importantly, however, we must recognize that the vast majority of consumers are unaware of these distinctions and consequently unaware of how their information may be handled under different regulatory requirements.

Another blurred distinction is whether information is "identifiable" or "de-identified." Information is increasingly difficult to classify as one or the other, particularly as it is copied, exchanged, or recombined with other information. Information once thought to be anonymized can be coupled with other datasets to determine an individual's identity. For example, geo-tagged information in anonymized craigslist postings were used to determine a person's name

---

[5] Markle Foundation. *Survey Snapshot: The Public and Doctors Agree on Importance of Specific Privacy Safeguards*. December 3, 2010. Accessed on January 17, 2011: http://www.markle.org/health/publications-briefs-health/1367-survey-snapshot-public-and-doctors-agree-importance-specific-privacy-safeguards.

[6] Markle Foundation. "CP1: Policy Overview, Markle Connecting for Health Common Framework for Networked Personal Health Information." June 2008. Accessed on January 21, 2011: http://www.markle.org/health/markle-common-framework/connecting-consumers/cp1.

and address when coupled with publicly available information.[7] "Anonymized" neurological images, used for medical research, can become revealing of an individual's identity through the use of readily available graphic software.[8] The HIPAA Privacy Rule is premised on the idea that individually identifiable health information must be protected. However, this distinction has been blurred with new uses of technology and greater availability of digital information. The FTC report recognizes several factors that have contributed to this breakdown based on their recent roundtable discussions.[9] Panelists discussed how the comprehensive scope of data collection and the growing ability to compile and crosslink "disparate bits of 'anonymous' consumer data from numerous different online and offline sources" could be used to uniquely identify and track consumers. One method involves "fingerprinting" a user's browsers through the unique combination of seemingly innocuous settings such as the operating system a consumer uses, font settings, and installed plug-ins. With rapidly evolving technologies and databases, it is more appropriate to describe a spectrum of "identifiability," rather than a binary classification of information as identifiable or not. The question is not whether de-identified information might be made re-identifiable, but rather which entities would be able to re-identify the information, how much effort they would have to expend, and what limits are placed on their ability to do so.[10]

A third category of blurred lines pertains to what might be considered parts of a person's clinical record versus health-related information generated in non-clinical settings. There are increasing opportunities for organizations to capture, combine, and share information to build health profiles about individuals by using data sets such as: IP addresses, cookies, and web beacons and similar technologies; search keywords; data from health-monitoring devices; prescriptions or over-the-counter medication purchases; food purchases; information published by

---

7 Friedland, Gerald and Sommer, Robin. *Cybercasing the Joint: On the Privacy Implications of Geo-Tagging*. Available at http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf.

8 Schimke, Nakeisha, Kuehler, Mary and Hale, John. "On Resolving the Privacy Debate in Deidentified Neuroimages." HealthSec 2010. http://www.usenix.org/events/healthsec10/tech/.

9 Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers; Preliminary Staff Report." 2010: p. 36.

10 Markle Foundation. "CT1: Technology Overview, Markle Connecting for Health Common Framework for Networked Personal Health Information." June 2008. Accessed on January 21, 2011: http://www.markle.org/health/markle-common-framework/connecting-consumers/ct1.

See also: Centers for Democracy and Technology. "Building a Strong Privacy and Security Policy Framework for Personal Health Records." July 21, 2010. Accessed on January 21, 2011: http://cdt.org/files/pdfs/Building_Strong_Privacy_Security_Policy_Framework_PHRs.pdf.

consumers about themselves (e.g., personal health record data entries, patient diary entries, consumer ratings, online community posts); and a plethora of health-related applications for smart phone and tablet devices.[11]

These examples of "blurring lines"—which are by no means exhaustive—require that government and industry clearly articulate what is required to support consumer privacy and information protection in our connected world.

As the FTC's mission articulates,[12] industry practices must not be misleading or unfair. Misleading practices include misrepresentations or omissions that may contribute to a reasonable consumer's decision to use a service, provide personal information, or grant permissions relating to that data.[13] Unfairness may occur when consumers are injured after being forced or coerced into making decisions in the marketplace that are not their own.[14] The marketplace in our emerging connected world should be based on trusted and transparent relationships, without behind-the-curtain collections, uses, or disclosures of personal information that would catch an average consumer unaware. It would be alarming for consumers, as well as all legitimate network participants, if consumer data streams were harnessed by "shadow" businesses that exploit indirect and involuntary relationships with consumers.

---

[11] Markle Foundation. "CT1: Technology Overview, Markle Connecting for Health Common Framework for Networked Personal Health Information." June 2008. Accessed on January 21, 2011: http://www.markle.org/health/markle-common-framework/connecting-consumers/ct1.

[12] 15 U.S.C. § 45(a)

[13] Letter from FTC to Hon. John D. Dingell, Chairman, Subcommittee on Oversight and Investigations. October 14, 1983. Reprinted in appendix to Cliffdale Associates, Inc., 103 F.T.C. 110, 174, 1984. Accessed online on January 24, 2011: http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[14] Letter from the Federal Trade Commission to Hon. Wendell Ford and Hon. John Danforth, Senate Committee on Commerce, Science and Transportation. December 17, 1980. "Unfairness Policy Statement," appended to International Harvester Co., 104 F.T.C. 949, 1984. Accessed online on January 24, 2011: http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

A Coordinated Framework for Consumer Protection and Privacy

Looking ahead, we urge government to think less within historically defined sectors and more toward a construct that will fulfill common privacy expectations through the implementation of consistent requirements across relevant data holders. We submit that the following three guideposts will be crucial to the government's success in implementing and enforcing appropriate rules to protect consumer privacy.

1. *It is imperative to translate and specify FIPs in the context of personal health information.*

We support the FTC and Department of Commerce's embrace of Fair Information Practice Principles as a framework for consumer protection. Principles are merely the starting point, however. Any information-collection or information-sharing effort must translate the principles into specific policies, practices, and technology approaches that fit the context and that, when taken together, comprehensively protect privacy and data security.

This is precisely the approach we took to develop the Markle Common Framework for Networked Personal Health Information, defining a set of consistent and specific policies and practices for entities offering consumer facing personal health applications and services, regardless of whether they would be considered HIPAA covered. The table below (Table 1) illustrates how we translated a set of principles based on FIPs into specific recommended policy and technology practices for services that handle personal health information on behalf of consumers, including data flows in or out of electronic personal health records (PHRs).

Table 1: Translation of a set of principles based on the FIPs into specific policy and technology practices for services that handle personal health information.

Principle Based on FIPs	Translation into Specific Practices
Openness and Transparency • Is it easy to understand what policies are in place, how they were determined, and how to make inquiries or comment? • Is it clear who has access to what information for what purpose?	• Specific recommendations on how policy notices should be easily accessible, clear, comprehensive, summarized, and updated. • The consumer should be able to know what, how, and why information is collected, used, or shared, as well as how long it will be kept, how the consumer can exercise choices or controls over the information, and whether it can be disputed or deleted. • Policy notice is necessary, but not sufficient protection. Many consumers don't read notices, so a full trust framework is necessary. **See Markle Common Framework:** • CP2: Policy Notice to Consumers[15]
Purpose Specification and Minimization • What is the purpose of gathering these data? • Are the purposes narrowly and clearly defined?	• The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes. • Each occasion of change of purpose requires further notice and, if warranted, consent. **See Markle Common Framework:** • CP2: Policy Notice to Consumers • CP3: Consumer Consent to Collections, Uses, and Disclosures of Information[16]
Collection Limitation • Are only those data needed for the specified purposes being collected?	• Specific recommendations to ensure that personal health information is collected only for specified purposes and should be obtained by lawful and fair means. • The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. (For example, if it's only necessary to know a person's age, it's not necessary to collect or share the date of birth.) **See Markle Common Framework:** • CT4: Limitations on Identifying Information[17]

[15] http://www.markle.org/health/markle-common-framework/connecting-consumers/cp2

[16] http://www.markle.org/health/markle-common-framework/connecting-consumers/cp3

[17] http://www.markle.org/health/markle-common-framework/connecting-consumers/ct4

Principle Based on FIPs	Translation into Specific Practices
Use Limitation • Will the data only be used for the purposes stated and agreed to by the subjects?	• Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified. • It is important to disallow discrimination based on information in PHRs or similar consumer health information tools. • Participating organizations should take a strong stand against "compelled disclosures" (i.e., when consumers must allow organizations access to personal information in their PHR as a condition of employment, benefits, or other critical services.) **See Markle Common Framework:** • CP7: Discrimination and Compelled Disclosures[18] • CT4: Limitations on Identifying Information
Individual Participation and Control • Can an individual find out what data has been collected and exercise control over whether and with whom it is shared?	• Consumers should also be able to review and exercise controls over the way their information is being used, stored, or shared. • Consumers should be notified if they are affected by an information breach. • Data collections, uses, or disclosures of personal information that could be particularly sensitive or unexpected by a reasonable consumer, or any that pass the user's personally identifiable information to unaffiliated third parties, should be subject to additional consent and permissions (i.e., independent consent), which should be obtained from users in advance of the use or disclosure. **See Markle Common Framework:** • CP3: Consumer Consent to Collections, Uses, and Disclosures of Information • CP5: Notification of Misuse or Breach[19] • CP7: Discrimination and Compelled Disclosures • CP8: Consumer Obtainment and Control of Information[20] • CT3: Immutable Audit Trails[21] • CT5: Portability of Information[22]

[18] http://www.markle.org/health/markle-common-framework/connecting-consumers/cp7

[19] http://www.markle.org/health/markle-common-framework/connecting-consumers/cp5

[20] http://www.markle.org/health/markle-common-framework/connecting-consumers/cp8

[21] http://www.markle.org/health/markle-common-framework/connecting-consumers/ct3

[22] http://www.markle.org/health/markle-common-framework/connecting-consumers/ct5

Principle Based on FIPs	Translation into Specific Practices
Data Integrity and Quality • How are the data kept current and accurate?	• All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date. **See Markle Common Framework:** • CP6: Dispute Resolution[23] • CP8: Consumer Obtainment and Control of Information • CT2: Authentication of Consumers[24] • CT3: Immutable Audit Trails
Security Safeguards and Controls • How are the data secured against breaches, loss, or unauthorized access?	• Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure. **See Markle Common Framework:** • CP5: Notification of Misuse or Breach • CT2: Authentication of Consumers • CT4: Limitations on Identifying Information • CT6: Security and Systems Requirements[25] • CT7: An Architecture for Consumer Participation[26]
Accountability and Oversight • Who monitors compliance with these policies? • How is the public informed about violations?	• Entities in control of personal health information must be held accountable for implementing these principles. **See Markle Common Framework:** • CP4: Chain-of-Trust Agreements[27] • CP5: Notification of Misuse or Breach • CP6: Dispute Resolution • CP9: Enforcement of Policies[28] • CT3: Immutable Audit Trails

[23] http://www.markle.org/health/markle-common-framework/connecting-consumers/cp6

[24] http://www.markle.org/health/markle-common-framework/connecting-consumers/ct2

[25] http://www.markle.org/health/markle-common-framework/connecting-consumers/ct6

[26] http://www.markle.org/health/markle-common-framework/connecting-consumers/ct7

[27] http://www.markle.org/health/markle-common-framework/connecting-consumers/cp4

[28] http://www.markle.org/health/markle-common-framework/connecting-consumers/cp9

Principle Based on FIPs	Translation into Specific Practices
Remedies • How will complaints be handled? • Will consumers be able to respond to or be compensated for mistakes in decisions that are based upon the data?	• Remedies must exist to address security breaches or privacy violations. **See Markle Common Framework:** • CP5: Notification of Misuse or Breach • CP6: Dispute Resolution • CP9: Enforcement of Policies

Only when taken as a whole do these principles and related practices constitute a trust framework. Elevating certain principles over others will weaken the overall protection of consumers. The consequences of elevating certain principles over others are especially relevant to the limitations of the "notice and choice" model—a key element of FTC's early privacy work. The FTC describes how over the years businesses have not adequately informed consumers of how their information would be used and have not offered consumers adequate ability to control such practices. As detailed by the FTC, the net effect of this is that privacy policies have become longer, more complex, and often incomprehensible to consumers. As a result, consumers face a substantial burden in reading and understanding privacy policies and exercising the limited choices that they have. Without developing a more complete set of protections, over-reliance on "notice" results in weak protection. This is a very precise example of why no one principle should be emphasized over others.

2. Coordination of federal privacy efforts is critical.

Several federal agencies have a key role to play in consumer health information privacy policy development and enforcement. It is critical that agencies and departments throughout the federal government coordinate their roles and responsibilities so that, whenever possible, consistent requirements can be applied to offer meaningful protections to consumers, and to avoid unnecessary confusion in the marketplace. An example of potential problems that can arise due to inconsistency is in the area of breach notification, where rule-writing under HITECH led to different standards between the Department of Health and Human Services

(HHS) and FTC. Markle Connecting for Health collaborators addressed foreseeable conflicts in the rules in collaborative comments.[29]

HITECH calls for HHS and FTC to implement regulations requiring that individuals be notified if a security breach compromises their personal health information. HHS was required to implement regulations for Covered Entities and Business Associates subject to HIPAA, while FTC was required to implement regulations for PHRs and PHR-related applications. Because the two rules do not address breach notification in the same manner, the average consumer is unlikely to know which rules apply to which services.

Because the health care sector is rapidly evolving through the emergence of new Internet-enabled technologies and services, it is increasingly important for consumer privacy and data protection policies to be coordinated across federal agencies and departments. In developing a framework for consumer protection and data privacy, the FTC and Department of Commerce must coordinate with HHS, particularly, with the Office of the National Coordinator for Health Information Technology (ONC), and the Office of Civil Rights (OCR). Recently, these bodies have engaged in collaborative efforts with the FTC by holding a PHR Roundtable to help inform ONC's congressionally mandated report on privacy and security requirements for Non-Covered Entities. The report will examine which federal government agency is best equipped to enforce such requirements. In finalizing their recommendations to Congress, it will be instrumental for consumer trust that the agencies recognize the need for consistency wherever possible in the requirements for protecting a consumer's personal health information.

3. *Looking ahead, to meet consumer expectations, policy development must take a coordinated approach to privacy and security protections, rather than proceeding solely on a sector-by-sector basis.*

An erosion of trust could inhibit the adoption of new technologies. Adopting a coordinated approach to privacy and security across federal policy development could help support innovation and novel consumer services. In the long run, if federal policy is only developed for the protection of consumer information sector-by-sector, then consumers will not know what to

---

[29] Markle Foundation, et al. Markle Collaborative Comments: *Objective Standards Needed for Evaluating Breaches, HITECH Breach Notification for Unsecured Protected Health Information Rulemaking*. October 23, 2009. Accessed on Web January 23, 2011: http://www.markle.org/publications/837-objective-standards-needed-evaluating-information-breaches.

expect from companies that do not fall neatly into a given sector for a given service. The federal government should contemplate a 21st century coordinated policy-development model to address a future of increasingly blurry lines of commercial uses of consumer health information and to avoid balkanizing policy development solely within previously defined sectoral or agency boundaries.

Going forward, we urge the federal government to think of privacy more from the consumer perspective. Supported through further collaboration and coordination among agencies and departments, as well as the private sector, it is critical to fulfill the expectations consumers have for trust based on consistent protections of privacy across an increasingly connected world where their interactions get more complex and the collections and uses of their information evolve with the emergence of new services and intermediaries. Consumers should have a clear understanding of the protections surrounding their personal information, and industry must have a clear understanding of consistent rules of the road if it is to earn and keep the public's trust.

CC: The Honorable Gary Locke
Secretary, Department of Commerce

The Honorable Kathleen Sebelius
Secretary, Department Of Health and Human Services

Georgina Verdugo
Director, Office for Civil Rights
Department Of Health And Human Services

David Blumenthal, MD, MPP
National Coordinator for Health Information Technology, Office of the National Coordinator for Health Information Technology
Department Of Health And Human Services

This letter was formulated by a collective view informed by many and diverse collaborators within the Markle Connecting for Health community, and is supported by the following individuals and organizations.*

Christine Bechtel
National Partnership for Women & Families

Hunt Blair*
Office of Vermont Health Access

Jennifer Covich Bordenick
eHealth Initiative

Adam Bosworth
Keas, Inc

Jeff Brown
Wal-Mart Stores, Inc.

Warwick Charlton, MD
Intuit Health

Mark Chassin, MD, MPP, MPH
The Joint Commission

Steven Findlay, MPH
Consumers Union

Mark Frisse, MD, MBA
Vanderbilt University

Gilles Frydman
Association of Cancer Online Resources

Daniel Garrett
PricewaterhouseCoopers LLP

Douglas Gentile, MD, MBA
Allscript

Adrian Gropper, MD
MedCommons

Jim Hansen
Dossia Consortium

Joseph Heyman, MD
Whittier Independent Practice Association

Gerry Hinkley, JD
Pillsbury Winthrop Shaw Pittman LLP

Michael B. Jackson
Adobe Systems, Inc.

William F. Jessee, MD
Medical Group Management Association

Joseph Kvedar, MD
Center for Connected Health, Partners HealthCare System, Inc.

David Lansky, PhD
Pacific Business Group on Health

Jack Lewin, MD
American College of Cardiology

Philip Marshall, MD, MPH
Press Ganey Associates, Inc.

Deven McGraw, JD, MPH
Center for Democracy and Technology

Howard Messing
MEDITECH

* *Federal, state, and city employees collaborate but make no endorsement.*

Peter Neupert
Microsoft Corporation

Margaret E. O'Kane
National Committee for Quality Assurance

J. Marc Overhage, MD, PhD
Regenstrief Institute, Inc.;
Indiana Health Information Exchange

Herbert Pardes, MD
NewYork-Presbyterian Hospital and
NewYork-Presbyterian Healthcare System

Amanda Heron Parsons, MD, MBA*
New York City Department of Health &
Mental Hygiene

Peter Schad, PhD
RTI International

Scott Schumacher, PhD
IBM

Raymond Scott
Axolotl

Thomas Sullivan, MD
DrFirst

Paul Tang, MD
Palo Alto Medical Foundation

John Tooker, MD, MBA, MACP
American College of Physicians

Paul Uhrig, JD
Surescripts

Robert Wah, MD
American Medical Association
Computer Sciences Corporation

Markle Foundation

Zoë Baird
President

Carol C. Diamond, MD, MPH
Managing Director, Health
Chair, Markle Connecting for Health

* *Federal, state, and city employees collaborate but make no endorsement.*