The Preliminary FTC Staff Report – Implications for Healthcare Businesses.

The Federal Trade Commission (FTC) has jurisdiction over for-profit entities,[1] including those whose activities include the collection, use, maintenance and disclosure of consumers' private healthcare information. All such entities should be aware of the framework recently created by the FTC for the protection of such consumers' private health information. Moreover, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies specifically to the collection, use and disclosure of health information by HIPAA covered entities which include health care providers, health plans, health care clearinghouses and their business associates.[2] Many of those covered entities and business associates are for-profit entities that fall under the jurisdiction of the FTC. Healthcare businesses that collect private health information are advised to review their policies and internal monitoring operating procedures to ensure compliance with FTC guidance on the protection of consumer information, regardless of whether they are required to protect private health information as a covered entity under HIPAA.

In December 2010, the FTC issued a preliminary staff report[3] intended to initiate a standardizing framework for how businesses should ensure the privacy of consumer information they collect and/or maintain (the "Framework"). The Framework serves as guidance for policymakers, including members of Congress, as they continue to resolve

[1] See FTC Act, 15 U.S.C. §§44 and 45, http://www.ftc.gov/ogc/stat1.shtm.
[2] 45 C.F.R. pt. 160, http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr160_07.html, and subpt. A & E pt. 164 http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr164_07.html.
[3] FEDERAL TRADE COMMISSION, A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS: PRELIMINARY FTC STAFF REPORT (2010) [hereinafter FRAMEWORK], http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. The Commission expects to issue a final report later this year.

the ever expanding issues that relate to privacy and data security.[4] The Framework is also meant to guide companies in the creation of "effective best practices" as they formulate their own internal administrative and technological procedures to protect consumer privacy.[5]

The FTC has been involved with the protection of health information since before the Framework was released. The American Recovery and Reinvestment Act of 2009 ("ARRA") recognized new types of web-based entities that collect consumers' health information including vendors of personal health records and online applications that interact with such personal health records. Many of these entities are not subject to the privacy and security requirements of HIPAA. ARRA required the FTC to issue regulations implementing a requirement that such entities notify individuals in the event of a security breach with respect to their health records. On August 25, 2009, the FTC issued the Health Breach Notification Rule.[6] The rule requires each vendor of personal health records and each PHR related entity[7] to notify each individual whose unsecured PHR identifiable health information[8] is acquired by an unauthorized person as a result of such breach of security and to also notify the FTC of such breach.

---

[4] FRAMEWORK, at i (Executive Summary), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[5] *Id.*
[6] 74 Fed. Reg. 42962 (codified at 16 C.F.R. pt. 318), http://www.ftc.gov/os/2009/08/R911002hbn.pdf.
[7] "PHR related entity" means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity that: (1) Offers products or services through the Web site of a vendor of personal health records; (2) Offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records; or (3) Accesses information in a personal health record or sends information to a personal health record. 16 C.F.R. § 318.2(f), http://www.ftc.gov/os/2009/08/R911002hbn.pdf.
[8] "PHR identifiable health information" means 'individually identifiable health information,' as defined in section 1171(6) of the Social Security Act (42 USC 1320d(6)), and, with respect to an individual, information: (1) That is provided by or on behalf of the individual; and (2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. 16 C.F.R. § 318.2(e), http://www.ftc.gov/os/2009/08/R911002hbn.pdf.

Proposed Framework Applicable to All Commercial Entities that Collect or Use Consumer Data, including Health Care Data.

The principles of the Framework are applicable "to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device."[9]

The proposed Framework also governs information gathered in both the online and offline context regardless of whether there was a direct interaction with the actual consumer.[10] In the healthcare privacy context there are many implications for pharmaceutical companies, advertising companies, as well as data brokers that may be utilized by health insurers.

Three Core Principles of the Framework: Privacy by Design; **Simplified Choice; and Greater Transparency**

Reflecting the concepts of the Federal Trade Commission Act (the "FTC Act"), as well as federal, state, and international law and guidelines concerning privacy,[11] the Framework is comprised of three core principles: (1) Privacy by Design; (2) Simplified Choice; and (3) Greater Transparency.

I. **Privacy by Design:**

[9] FRAMEWORK, at 42, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[10] *Id.*
[11] FRAMEWORK, at 39.

The FTC puts forth the idea that businesses should incorporate and promote privacy considerations at every stage of the development of their products and services.[12] Businesses can accomplish this by instituting concrete privacy protections, such as the elements of data security, reasonable collection limits, sound retention practices, and data accuracy.[13]

Privacy by Design Element 1: Data Security

First, businesses that collect the personal information of consumers that includes health information, should utilize reasonable physical, technical, and administrative safeguards.[14] The standards that should be utilized when developing these should be based on the safeguards rule of the Gramm-Leach Bliley (GLB) Act (the "Safeguards Rule").[15]

The GLB Act sets out the data security requirements for financial institutions[16] and the Safeguards Rule provides that financial institutions "shall develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical and physical safeguards" that correlate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue.[17]

---

[12] *Id.* at 44, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[13] *Id.*
[14] *Id.* at 44-45.
[15] 67 Fed. Reg. 36484 (May 23, 2002) (codified at 16 C.F.R. pt. 314), http://www.ftc.gov/os/2002/05/67fr36585.pdf.
[16] 15 U.S.C. § 6801(a), http://www.ftc.gov/privacy/glbact/glbsub1.htm#6801.
[17] 16 C.F.R. § 314.3, http://www.ftc.gov/os/2002/05/67fr36585.pdf.

The FTC utilized the elements of the Safeguards Rule in recent multi-million dollar settlements between the FTC and CVS/Caremark[18] & Rite-Aid.[19] In both instances, the pharmaceutical retailers discarded materials containing personal information such as pharmacy labels and employee Social Security Numbers in publicly accessible dumpsters. Even though the companies represented that they implemented reasonable and appropriate measures to protect personal information against unauthorized access, they were found not to have done so.[20] The FTC viewed this as a violation of Section 5 of the FTC Act, and subsequently imposed hefty fines and mandatory internal corrective action. Thus it is advisable that all affected healthcare businesses utilize the elements of the Safeguards Rule to protect consumer privacy.

Privacy by Design Element 2: Reasonable Collection Limits

The second element of privacy by design provides that companies should "collect only the information needed to fulfill a specific legitimate business need."[21] For example, if the primary goal of an advertising network is to track consumers' online activities to serve targeted ads, there is no need for the network to track all keystrokes of the consumer or use other applications to capture all data that a consumer inputs.[22] This extra information is not necessary in assisting the advertising network in achieving its primary goal.

---

[18] In re CVS/Caremark Corp., Decision and Order, F.T.C., File No. 072-3121 (2009), *available at* http://www.ftc.gov/os/caselist/0723119/090623cvsdo.pdf.
[19] In re Rite Aid Corp., Agreement Containing Consent Order, F.T.C., File No. 072-3121 (2010), *available at* http://www.ftc.gov/os/caselist/0723121/100727riteaidagree.pdf.
[20] *See* In re CVS/Caremark Corp., Complaint, F.T.C., Docket No. C-4259 *available at* http://www.ftc.gov/os/caselist/0723119/090623cvscmpt.pdf *and* In re Rite Aid Corp, Complaint, F.T.C., Docket No. C- *available at* http://www.ftc.gov/os/caselist/0723121/100727riteaidcmpt.pdf.
[21] FRAMEWORK, at 45-46, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[22] *See id.* at 46 for other examples including: "[i]f a mobile application is providing traffic and weather information to a consumer based on his or her location information, it does not need to collect contact lists or call logs from the consumer's device."

Privacy by Design Element 3: Sound Retention Practices

The third element of creating privacy by design is the consideration of the length of time a company holds the information it collects. "[C]ompanies should implement reasonable and appropriate data retention periods, retaining consumer data for only as long as they have a valid business need to do so."[23]

Retention time is particularly important for businesses that collect health information. For example, smart phones can provide access to geolocational data. It can maintain the location information about a patient's repeated visits to a health care provider. If that health care provider only treats cancer patients, sensitive information "about that consumer's health that would otherwise be private" could potentially be divulged.[24] Maintaining this old data over time could create a detailed health history of a consumer in addition to possibly identifying him. Therefore, companies should retain consumer information only as long as they have a valid business need to do so or as otherwise required by law.

Privacy by Design Element 4: Data Accuracy

The fourth element of creating privacy by design is the need to ensure that the information that companies collect is accurate.[25] This is of particular importance if that information is later utilized to "deny consumers benefits or cause significant harm."[26] For example, erroneous information regarding a consumer's preexisting conditions or

---

[23] *Id.*
[24] PROPOSED FRAMEWORK, at 47, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[25] *Id.* at 48, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[26] *Id.*

financial history may affect the ability to obtain affordable health insurance. Therefore, it is crucial that companies build in safeguards to ensure that the information they collect is accurate.

Privacy by Design - Comprehensive Data Management Procedures

In order to ensure that the above elements of data security, reasonable collection limits, sound retention practices, and data accuracy are properly incorporated by businesses, the FTC recommends that companies "maintain comprehensive data management procedures throughout the life cycle of their products and services."[27] This should be an integral part of the business model. This is of particular importance when the business collects personal, identifiable information and other sensitive data. Some ways that comprehensive data management may be achieved are:[28]

1. Designating specific personnel who are responsible for training employees on privacy as well as promoting accountability for privacy policies throughout the organization.

2. Staying abreast on new developments in privacy law so that internal business policies and practices may be modified to be in accord with these changes.

3. Utilizing new technologies that assist in providing increased protection of sensitive data.

[27] *Id.* at 49.
[28] *See id.* at 49-52.

Because the concepts of the privacy by design principle may be particularly difficult to implement for businesses that maintain personal health records utilizing legacy data systems,[29] it may be beneficial for the FTC to offer incentive programs similar to initiatives instituted to get health care providers to utilize EHR.[30]

Second Core Principle- Simplified Choice:

The second core principle of the Framework is that companies should simplify the method by which consumers elect whether to have their information collected, used, or shared.[31] Consumers are often presented with lengthy privacy policies that may be difficult to comprehend and effectively meaningless where the consumer is not provided with the opportunity to fully understand them. Moreover, businesses are burdened in the creation of lengthy policies that may be of minimal benefit to the end user. The report suggests a simplified choice model with the goal of providing consumers with meaningful choice while setting forth a limited set of data practices for which consumer choice is not necessary, thereby also reducing the burden on companies.

Simplified Choice - No Need to Provide Choice for Certain Commonly Accepted Practices

The Framework provides that once a consumer chooses to use a product or service, companies do not need to provide choice before collecting and using consumers'

[29] In this context a legacy data system is an older form of technology that is still in use even though there are newer, more streamlined versions available.
[30] As part of the ARRA of 2009, CMS implemented a program that provides monetary incentives for eligible professionals, hospitals, and critical access hospitals that are meaningful users of EHR. *See* CMS.gov, EHR Incentive Programs, http://www.cms.gov/EHRIncentivePrograms/01_Overview.asp#TopOfPage.
[31] FRAMEWORK, at 53.

data for "commonly accepted practices."[32] The commonly accepted practices enumerated by the FTC are:[33]

(1) Product and service fulfillment;

(2) Internal Operations;

(3) Fraud prevention;

(4) Legal compliance and public purpose; and

(5) First party marketing.

Sensitive information, such as medical information, however, warrants special protection.[34] The Framework suggests that before such data is collected, used, or shared, consumers should provide affirmative express consent.[35]

Further guidance related to privacy and consent was recently provided by the United States Supreme Court. In *Sorrel v. IMS Health Inc*.,[36] the Court decided that the First Amendment does not allow a state to prevent pharmaceutical companies that have received a prescriber's data as a third-party, from utilizing the information to subsequently market specific drugs to doctors.[37] Specifically, the Court held that the Vermont statute unconstitutionally burdened the speech of pharmaceutical marketers and

[32] Commission staff came up with a limited set of "commonly accepted practices" that should be subject to consumer choice, for example routine data backups. *See* FRAMEWORK, at 53, note 132, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[33] *Id.* at 53-54.
[34] Other information considered sensitive includes information about children, financial, and geolocational data. FRAMEWORK, at 61.
[35] *Id.*
[36] *Sorrell v. IMS Health Inc*., 630 F.3d 263 (2d Cir. 2010), *cert. granted* (U.S. Jan. 7, 2011), *aff'd* (No. 10-779 June 23, 2011), http://www.supremecourt.gov/opinions/10pdf/10-779.pdf.
[37] *Id.*

data miners without adequate justification.[38] This case presents numerous privacy concerns for both the doctor and the patient. For the doctor, information about their prescribing habits could be utilized by individuals looking to "doctor shop" or gain access to medications for recreational rather than therapeutic use. For the patient, an individual can be re-identified via a combination of sources[39] and thus their sensitive health information could arguably become public.

Simplified Choice – Where choice is required, the company should offer such choice at the appropriate time and in the appropriate context

The Framework would require companies to give consumers the ability to make informed and meaningful choices where the activity of the company does not fall within the "commonly accepted practices." For example, Company A, a retailer, collects purchase information directly from the consumer. Company A then sells the collected consumer information to a data broker or other third-party that may be unknown to the consumer. Because this is not a "commonly accepted practice," Company A must provide the consumer with the opportunity to make an informed and meaningful choice with respect to the collection and use of their information.

The Framework states that companies should describe consumer choices clearly and concisely, and offer easy-to-use choice mechanisms.[40] The choice mechanism

[38] *Id.*
[39] *See* supra note 24 and accompanying text regarding geolocational data. If information regarding a patient's visits to the doctor is stored, and that doctor is known as an infectious disease doctor specializing in HIV based on his prescribing habits, "piecing" together that information could potentially re-identify the patient.
[40] FRAMEWORK, at 57, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

should be offered at a[41] time and in a context in which the consumer is making a decision about his or her data.

Third Core Principle - Greater Transparency:

The final principle of the Framework is that "companies should increase the transparency of their data practices."[42] This principle is underscored by a "Complaint, Request for Investigation, Public Disclosure, Injunction, and Other Relief" (the "Advocates' Complaint") filed with the FTC in November 2010 by the Center for Digital Democracy, U.S Public Interest Research Group, Consumer Watchdog and the World Privacy Forum (the "Consumer Advocacy Groups").[43] The Advocates' Complaint requests that the FTC "conduct an investigation and public accounting of how pharmaceutical and online health services engage in data-collection practices, including behavioral tracking, used for profiling and targeting."[44] Specifically, the Consumer Advocacy Groups request that the FTC create "clear consumer protection safeguards" to protect health information and address the variety of marketing techniques utilized by health-related companies to target consumers.[45] The Consumer Advocacy Groups argue that the privacy policies currently available on health related websites fail to provide the

[41] *Id*.
[42] FRAMEWORK, at 69.
[43] In re Online Health and Pharmaceutical Marketing that Threatens Consumer Privacy and Engages in Unfair and Deceptive Practices, Complaint, Request for Investigation, Public Disclosure, Injunction, and Other Relief, F.T.C., (Nov. 19, 2010), *available at* http://www.democraticmedia.org/sites/default/files/2010-11-19-FTC-Pharma-Filing.pdf.
[44] *Id.* at 10-11.
[45] *Id.* at 6, http://www.democraticmedia.org/sites/default/files/2010-11-19-FTC-Pharma-Filing.pdf.

consumer with substantive information regarding how personal information about their medical conditions are used and collected.[46]

Currently, the Framework addresses the issue of transparency by suggesting that:

i) Privacy notices should be clearer, shorter, and more standardized, to provide better understanding for the consumer and the ability to conduct a meaningful comparative analysis of privacy practices.[47]

ii) Businesses should have appropriate methods for consumers to have reasonable access to their individual data.[48]

iii) If a company makes a material change to their policies and procedures, that subsequently changes how a consumer's information may be later used and/or collected, the company "must provide prominent disclosures and obtain affirmative express consent."[49]

iv) All stakeholders play a collective role in informing and educating consumers about commercial data practices.[50]

Conclusion

The FTC Framework applies to all for-profit entities whose activities include the collection, use, maintenance and disclosure of consumers' private healthcare information. These entities should be aware of and implement the Framework with respect to their

[46] *Id.* at 11.
[47] FRAMEWORK, at 70, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[48] *Id.*
[49] FRAMEWORK, at 77.
[50] FRAMEWORK, at 78.

business activities. Additionally, because many of the HIPAA covered entities are also for-profit entities, these entities should dually comply with the FTC Framework and HIPAA.

At a time when breaches of data security and non compliance with privacy law can mean large fines[51] it is imperative for businesses that collect, maintain, use or disclose health records institute stringent initiatives that ensure that the sensitive information of their consumers remain private. By implementing the best practices described in the Framework, businesses that collect health information will also be less likely to experience a breach involving health information necessitating reporting pursuant to the FTC Health Breach Notification Rule.

[51] *See supra* notes 18-20 and accompanying text.

MOSES & SINGER LLP

Disclaimer

Viewing this or contacting Moses & Singer LLP does not create an attorney-client relationship.

This is intended as a general comment on certain developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This contains information that may be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

Attorney Advertising

It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.