KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org
CENTER FOR DEMOCRACY
& TECHNOLOGY

May 5, 2015

Statement of Michelle De Mooy
Deputy Director, Consumer Privacy Project
Center for Democracy & Technology

Before the Subcommittee on Privacy, Confidentiality & Security
National Committee on Vital and Health Statistics
United States Department of Health and Human Services

Section 1179 of the Health Insurance Portability and Accountability Act

Dear Subcommittee Members,

Thank you for the opportunity to testify on behalf of the Center for Democracy and Technology. CDT is a nonpartisan, non-profit technology policy advocacy organization dedicated to protecting civil liberties and human rights on the Internet, including privacy, free speech, and access to information. I currently serve as the Deputy Director of CDT's Consumer Privacy Project, which focuses on developing privacy safeguards for consumers through a combination of legal, technical, and self-regulatory measures. Ensuring that services are designed in ways that preserve privacy, establishing protections that apply across the life cycle of consumers' data, and giving consumers control over how their data is used are key elements of protecting privacy in the digital age.

We welcome the Subcommittee's work on the applicability of Section 1179 of the Health Insurance Portability and Accountability Act (HIPAA) to financial institutions in today's rapidly evolving global marketplace.

Overview

Consumers are increasingly curating and controlling their own health and medical information across a wide variety of platforms. They are using personal health record tools to access and copy health records and move them to third party platforms, sharing health information on social networking sites, and leaving digital health footprints when they conduct online searches for health information. The health data created, accessed, and shared by consumers using these and many other tools can range from detailed clinical information, such as downloads from an implantable device and details about medication regimens, to data about weight, caloric intake, and exercise logged with a smart phone app. This information is increasingly being used and shared in unexpected and impactful ways, such as through employee wellness programs. Wellness programs connected to life insurance, for example, provide data to many entities, some of which are unknown to the consumer. Programs using personal monitoring technologies like fitness trackers or apps send data to affiliates and business partners, all of which can be combined with other public or private data from places such as grocery stores or gyms. Though depending on the contractual arrangement, some data may be subject to federal law, in a large number of cases the only privacy rules that apply in this context are the ones

companies may, or may not, have set for themselves in their privacy policies.

All of these developments offer a wealth of opportunities for health care and personal wellness, as well as for businesses seeking new sources of revenue in the management and delivery of this information, with the added benefit of not having to incur compliance costs, as much of this type of data is accessed and used outside of traditional healthcare and beyond the scope of HIPAA.

As a larger volume of personal health data becomes available and accessible to healthcare providers, the need for data management and processing has skyrocketed. Banks and financial institutions have increasingly stepped in to fill this demand, seeking more ways to monetize their interaction with personal health data as their services evolve in support of the health industry, far beyond their traditional role as check processors.

Accounts receivable services for healthcare providers, for example, have evolved to include banks "mailing letters to patients who are behind on payment, reviewing the terms of coverage agreements and provider contracts with health plans and other payers and applying them in dealing with patients, setting up payment schedules, and tracing changes to patient addresses."[1] Many banks are choosing to employ third party administrators (TPA) in order to avoid being characterized as a business associate under HIPAA, and despite their covered-entities status not much is known about the actual businesses practices of TPAs. With so many banks now achieving "vertical integration" of their services, via the easing of regulations in this area, the lines between traditional banking and other services that involve customer data, such as banks that are integrated with broker dealers and consultancy practices, have been blurred. Combined with the rise of third party involvement, important questions about how customer health information is being collected, shared, and used are raised.

Banks are also meeting the increased need by providers to convert data into electronic formats and facilitate interoperability by processing PHI from a non-standard format to a standard electronic format for purposes of billing and claims payment, acting as automated clearinghouse (ACH) services under HIPAA. Banks also often provide lockbox services for health care clients, wherein providers can send paper checks to a secure place for processing, particularly helpful when banks clients are not able to accept online payments. Companies like PayPal, Square and ProPay Jak have entered the payment and process space for this and other services. In addition to electronic payment options, mobile payment services like Square offer providers the ability to send an email or text message receipts to patients while PayPal's invoicing service will manage and track payments for providers. The functions these service offer are closely related to bank services.

Privacy concerns

[1] Augsburger, M. (2013, Feb 13). *The Convergence of Health Care and Banking*. Retrieved Jan 11, 2014, from Health Care Law Matters: http://www.healthcarelawmatters.com/compliance/the-convergence-of-health-care-and-banking/

Section 1179 creates an exemption from compliance with HIPAA and accompanying rules when a financial institution is "engaged in authorizing, processing, clearing, settling, billing, transferring or collecting payments." If the statute is interpreted broadly, and banks are mostly exempt, privacy protections for consumers would exist primarily in the Gramm-Leach-Bliley (GLB) Act, the amendments to the Fair Credit Reporting Act made by the Fair and Accurate Credit Transactions Act (FACT Act), and through enforcement actions by the Federal Trade Commission (FTC). The question is, do these laws provide adequate protection for health information?

Far from being a privacy law, the GLB Act was intended to facilitate the integration of banks and other financial institutions that have almost nothing to do with health or medical information. The law permits financial institutions to disclose nonpublic personal information to other companies but requires these entities to inform people about such data practices and provide them with the ability to opt-out of some disclosures. Most people have little incentive to read the notices sent by these entities – not only are they difficult to parse, in the end, without collection and sharing limitations, a core complimentary element of notice – choice – is negated by the fact that these practices exist at most banks across the country. The ability to opt-out is also mitigated by the fact that federal and state laws implement these provisions somewhat differently depending on where the consumer lives.

Both HIPAA and GLB protect health information but under HIPAA individuals have far more rights, such as the right to access and correct their records or to view a list of disclosures. GLB does not allow for the possibility of confidential communication, as is available to consumers via HIPAA.

Generally, the FACT Act prohibits a bank and other creditors from obtaining and using health information for consumer-credit decision purposes, a worthy restriction. However, the law does not have a prohibition on the sale or sharing of personal health data with affiliates for marketing purposes, a key loophole that has been closed in HIPAA via the HITECH Act.

The FTC has been active in bringing enforcement actions against companies that violate the "unfair and deceptive" practices under their Section 5 authority, including numerous instances of the misuse of health information without proper consent.[2] However, the FTC is necessarily limited in it's power by a lack of key rulemaking authority in certain areas and by virtue of relatively small size considering its position as essentially the only cop on the privacy protection beat in the United States.

Recommendations: Section 1179

In general, banks providing lockbox services or accounts receivable services like the ones described above for their health care customers should still be considered business associates if the service performed requires the bank's use and disclosure of PHI to perform it. Mobile

[2] Federal Trade Commission, *In the Matter of PaymentsMD*, https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter

payment services like Square engaged to send email and text receipts to patients should likewise trigger a business associate relationship as outlined in the statute. In essence, when banks take extra steps in performing services for a health care institution—such as matching claims to receipts and identifying shortfalls on specific claims—then the exemption under Section 1179 should not apply.

Banks and financial institutions involved in these activities should have covered entity status as health care clearinghouses under the Privacy Rule, rather than less protective business associate agreements. In particular, we would recommend a rule mandating that the transmission of PHI through the banking system's ACH should be encrypted so that it is accessible only by the final recipient. Encryption would also help provide protection in the event of network security breaches as well as prevent potential data mining for marketing purposes.

Even when health data is not transferred to a third party, providers and payers should be wary of leveraging patient data on behalf of external entities, especially for marketing purposes.

Additionally, financial institutions providing services of any kind to healthcare providers should assess their activities through a lens of a business associate relationship to consider what the legal and regulatory compliance should look like. When a business associate agreement is in place, the current Privacy Rule already affords some flexibility for big data uses by permitting business associates to aggregate data from different covered entities, including data about the same patients in both sets, so long as covered entities do not receive back-identifiable information about persons who are not their patients. That limitation remains valid.

Likewise, HIPAA-covered entities should evaluate how they will treat financial institutions for compliance purposes, as Section 1179 is unclear whether hospitals, health insurers or other entities are relieved of their own compliance obligations when contracting with financial institutions. The Subcommittee should consider recommending that the Secretary issue guidance on the compliance obligations of covered entities contracting with financial institutions that are currently considered exempt but may be providing covered services under a new Section 1179.

Recommendations: Fair Information Practices

For providers and payers, the era of big data poses special considerations, as these entities increasingly may have the technical capacity to access external data sources about their customers. Doctors, other providers, and payers may increasingly seek access to health data generated by commercial gadgets and applications, such as Jawbone and Fitbit, or may enter into partnerships with such device and application developers. They could potentially access commercial data broker services (which providers and payers may already use for fraud control, and to assess ability to pay, and eligibility for, certain forms of financial assistance) to collect information about individuals' lifestyle choices and habits to inform care decisions. Other challenges arise with respect to collection of data that is publicly shared on social media or is freely searchable on the web. There may be scenarios in the mental health field or other contexts where such information may be relevant to treatment or processing; however, if payers become more interested in this data as they become more involved in managing chronic

care, they should proceed cautiously, with full transparency and express consent, regardless of their covered entity status.

The Fair Information Practices (FIPs) offers guidance for some of these challenges. Despite the growing complexity of data flows within the health care field, the principle of openness (or transparency) is still relevant, both at the initial point of data collection, and whenever patient data is used in subsequent analysis.

Openness and transparency
As a fundamental principle, whenever data is collected about an individual, it should be clear to the individual what is being collected and how it will be used. Health care professionals who interact with patients are obligated to make sure that patients are informed about how their data will be used, including about the potential for secondary usage not directly related to the patient's treatment. The more unexpected or potentially objectionable a data collection or usage may be, the greater the obligation to explain the practice to the patient. As Omer Tene and Jules Polonetsky have noted, "transparency with respect to the logic underlying organizations' data processing will deter unethical, sensitive data use and allay concerns about inaccurate inferences."[3] This becomes particularly important in the context of an entity going from behind-the-scenes and exempt to one that is a covered entity with compliance expectations.

Especially with the advent of big data, as the volume and uses of data grow, and as the HIT ecosystem becomes increasingly complex, payers should reconsider what they disclose to customers and how. Essentially this means that, to build trust, improve accountability, and meet a customer's expectation, regulated entities may need to go beyond what HIPAA requires. One way to do this, again regardless of covered-entity status, is to include in the paper-based notices concrete information about what entities actually do with patient data such as identifying major categories of research or marketing that it uses for data. Beyond paper notices, payers and business associates that do not directly interface with patients should clearly describe their data practices in transparency statements available on their websites. Again, though few patients may directly access that information, but making it available to regulators, advocates, and interested patients will incentivize companies to adopt objectively reasonable business practices, and will serve as a basis for holding them accountable to those policies, which adheres to the principle of public notice in the FIPs.

True transparency may become more important because of another factor running in parallel with the development of the learning health care system: as more and more people move from employer-provided health insurance to purchasing individual plans – or, in the case of employer-provided insurance, being more financially responsible for the costs of care – they may end up with more of a typical consumer relationship with their health plans, and it will be in the interest of the health plans to become more transparent about their relationships with entities such as financial institutions to strengthen that relationship.

[3] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW J. TECH. & IP 239 (2013), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip.

Due to the intrinsic sensitivity of health information, commercial vendors have an obligation to clearly disclose data collection practices at a time and in a manner that is likely to be seen and acted upon by the user. Rather than serving only as the basis for user consent, the notices should include concrete, digestible information about what entities actually do with user data. The FTC has made it clear that, even where a registration process obtains express user consent, that consent will be invalid and the data collection illegal if the a reasonable consumer would not be likely to understand the scope of the data practices being conducted.[4]

Increasingly, it will be possible for companies with *no relationship* with a consumer to collect health information in public spaces; hypothetically, a sensor could be set up on a street corner to monitor the heart rates of passers-by in order to conduct a study of the general population, or potentially to target hypertension ads to relevant consumers. Due to the sensitivity of health information, we believe that it would not be appropriate to collect health information that could be tied back to an individual or a device used by an individual without having a relationship with that individual. In other words, there should be no clandestine collection of health data. Likewise, given the sensitivity of health data, we do not believe that any individual's experience (such as the advertising he receives) should be altered due to observed health information that was not deliberately provided.

Focused collection/ collection limitation
Especially considering the sensitivity of health information, limiting collection in the health app and device context remains of prime importance. While some proponents of big data argue that the full benefits of big data cannot be realized without unbridled collection, we believe that focused collection builds consumer trust, without which societally beneficial commercial applications that access and use health information are unlikely to be adopted.

Data integrity / access
The accuracy principle should apply not only to data but also to the analytic processes applied to data and the outcomes generated by such analytics. We believe that companies developing consumer apps and devices should ensure that consumers can easily access their data and copy it in portable formats.

Individual participation / control
Fundamentally, the decision to share or transmit health information generated by a commercial app or device must reside with the individual. When using a commercial app or device, users should feel that they control their data, rather than merely sending it off into the cloud to be analyzed, modified, and shared with third parties. By promoting user control, developers can also promote trust in their app or device, which is especially crucial in the health context.

Individual control is necessarily connected to the notions of transparency and notice discussed above. Secondary uses such as internal stability research and security development may not require individual control through authorization and re-authorization from users, but

[4] *Id.*

developers and manufacturers should institute strong internal audit and oversight procedures to prevent internal misuse.

Security

It is now well-established principle that any entity collecting individual data is responsible for protecting the security of that data. Recent high-profile breaches and enforcement actions by the FTC reemphasize the need for strong security. A reasonable program must address technical, administrative, and personnel measures, and must include regular auditing and frequent updating.

FTC interpretation of its Section 5 authority already requires reasonable security for all personal information, including health information. However, it is not clear that the need for strong data security has been sufficiently internalized by corporate decision-makers. One way to address this would be to require companies to have robust data security plans. This would require them to consider security threats, and to put into place reasonable measures proportionate to the security risk and the sensitivity of the health information.

Accountability / remedies

As the size and diversity of datasets grow, and as analytic techniques make it easier to re-identify data and draw inferences from seemingly innocuous data, internal and external accountability must play a larger role in protecting health data. Whenever data is illegitimately used or transferred — or reasonable security protections are not put into place — regulators and patients must be able to obtain compensation and punitive remedies from bad actors.

Currently, the Federal Trade Commission uses its basic authority to bring enforcement actions against companies that fail to adequately protect user data. The FTC has targeted companies that over-collect information which use data in ways or that are inconsistent with stated privacy policies or terms of service, and that fail to take reasonable steps to safeguard data. Undoubtedly, the FTC will bring enforcement actions on similar grounds in the health context. (The agency could be even more effective if it had wider authority to impose penalties for privacy violations.) State attorneys general also have investigative and enforcement powers.

Internally, in addition to having a robust security program, companies that handle health information should also have privacy processes in place to ensure that products are developed with privacy and the primacy of the user in mind. We have previously advocated for strong access controls that limit unauthorized access to personal health data; this is a vital step in promoting privacy.

Companies collecting health data should adhere to the Fair Information Practice Principles described above, and they should have processes in place to assess their compliance with their own rules, and as mentioned before, use the lens of the business associate agreement to determine their practices. They should also have formalized internal processes to ensure that privacy-conscious decisions are made through the lifecycle of the data, and that analytical decisions and determinations made using consumer-generated health data are accurate and fair.

Overall, it is critical for commercial entities that collect, use, and share personal health information to imbed strong privacy and security standards into their products and services in order to maintain customer trust, improve adoption and retention rates, and enable the myriad potential health benefits that can come from empowering consumers with their health data.