National Committee on Vital and Health Statistics (NCVHS)

Meeting of the Privacy, Confidentiality, and Security Subcommittee

Including Listening Session 2 on "Health Information Privacy and Security Beyond HIPAA"

November 28, 2017

Meeting Summary

Virtual WebEx Meeting

NCVHS Membership Present

Linda Kloss, MA, Subcomittee Chair*
Nicholas Coussoule*
Alexandra Goss
Richard Landen, MPH, MBA
Jacki Monson, JD*
Robert Phillips, Jr., MD, MSPH
Helga Rippen, MD, PhD., MPH, FACPM*
William Stead, MD, NCVHS Chair
Lee Cornelius, PhD, LCSW
*Subcommittee member

Staff Present

Rebecca Hines, MHS, Executive Secretary, NCHS
Rachel Seeger, MPA, MA, OCR, HHS, Lead Staff to the Subcommittee
Maya Bernstein, JD, ASPE, HHS
Geneva Cashaw, NCHS
Lorraine Doo, MSW, MPH, CMS
Katherine Jones, MS, NCHS
Marietta Squire, NCHS

Presenters

Frank Pasquale, University of MD
Leslie Francis, University of UT
Bennett Borden, Drinker Biddle
Kevin Stine, NIST
Brian Abe, NIST
Adam Greene, Davis Wright Tremaine

Others

Rose Li and Associates, Inc., Contractor
Bob Gellman, Consultant

Call to Order:

Linda Kloss, Chair, Subcommittee on Privacy, Confidentiality, and Security, reviewed the agenda and facilitated the introductions. She reviewed the purpose of the meeting and specified the following goals:

1. Identify and describe the changing environment and the risks to privacy and security of confidential health information; highlight promising policies, practices and technology;
2. Lay out integrative models for how best to protect individuals' privacy and secure health data uses outside of HIPAA protections while enabling useful uses, services and research;
3. Formulate recommendations for the Secretary on actions that HHS and other federal Departments might take; and
4. Prepare a report targeted toward health data stewards.

Linda Kloss reviewed the agenda and described the scope of the session as a "big picture" review to consider the following areas: Big data and expanding uses and users; cyber-security threats and approaches; personal devices and the "Internet of things"; laws and regulations; evolving technologies for privacy and security; and evolving consumer attitudes.

Ms. Kloss then introduced the panelists who provided their prepared remarks.

Frank Pasquale, Professor of Law, University of Maryland

Mr. Pasquale began by noting that the presentation is largely based on a 2014 article "Redescribing Health Privacy: The Importance of Information Policy." He expressed concern about the proliferation of data, health profiles, and health extracted information outside of HIPAA-protected realms and would like the Committee and the healthcare system, in general, to consider the situation in light of the goals for privacy law.

He noted that the current system tightly controls the degree of sharing, use, and collection of health information within the healthcare sector. But the use and transfer of data beyond the healthcare sector, in many respects, is a lot less stringent and more lenient. Mr. Pasquale added that there is a demand for this type of data even if it is not the best quality because of the reduced regulatory burdens associated with it.

The members discussed worst-case scenarios, including "runaway data" which is data, once gathered, that is shared and re-shared with no recourse or consequence, in a non-HIPAA-protected environment.

The presenter added that the non-HIPAA protected space often lacks privacy protection, ironically, because of trade secrecy protection of data brokers' collection and transfer of data.

Another critical question is data hygiene or laundering, where entities use certain types of data to make decisions about individuals. The ultimate detrimental effect is discrimination even though the data may be flawed or erroneously derived.

The presenter cited failure of the HITECH Act which placed responsibility on the FTC to be mindful of unfairness, deceptiveness, and potential liability for transfers of data not covered by HIPAA or a protected entity, but the limited staff and meager support reduced effectiveness. Furthermore, he expressed concern when programs use the information to "reward" good health practices, this can inadvertently allow discrimination of sicker and less healthy individuals.

Leslie Francis, Professor of Law and Philosophy, University of Utah

Ms. Francis noted the disturbing situation that is becoming more prevalent, where data that once was HIPAA-protected may no longer be included under "protected" categories. The constantly changing and evolving lines of demarcation can be confusing for consumers to recognize. Without special knowledge or awareness, the general public may be unaware of new interpretations that erode privacy protections or strip them altogether.

Ms. Francis continued by explaining why non-HIPAA covered entities are a problem. On the surface, they look remarkably similar to covered entities in providing health information that is as detailed and as sensitive as what HIPAA-covered entities have, and in some cases might seem even interchangeable. What's often not spelled out is that such organizations may be getting personal health information (PHI) from HIPAA-covered entities—in such cases, patients may not even realize that their PHI has been transferred and is no longer HIPAA-protected.

Registries, she noted, are repositories of patient data collected for specific purposes. Some of these involve patients with specific diseases, known exposures and/or specific treatments. Registries provide an example of data that trickles "downstream" collected and compiled from various sources, often the subject of sale, a mixture with large, big data sets, and potentially containing information that either came directly from patient records or indirectly through patient entry.

She then noted that even some existing protections, primarily at the FTC and some state laws, are uneven. The privacy policies and the terms of conditions that these entities have are not clear, are inconsistent, and confusing. She indicated particular concerns about dealing with de-identified information, especially among registries. Re-identification risks are relatively well known, but de-identified data is almost completely outside the regulatory requirements.

In some cases, information derived from conjoined datasets can yield unexpected or surprising inferences that can potentially be stigmatizing. If extrapolated to subpopulation groups, the results could be economically damaging, result in unfair workplace policies, job loss, or redlining to deprive groups of various benefits.

Ms. Francis noted that security protections are very uneven at this time as are data governance practices including data use agreements—unless decent enforcement is assured.

Bennett Borden, Partner, Drinker Biddle

In his presentation, Mr. Borden indicated that the volume, velocity and variety of data is expanding, especially with the increasing use of internet connected devices and the internet of things. He noted that we are collecting information about ourselves in ways that were unimaginable just a few years ago. Data is being collected and shared with wearables, implantables and even embedded devices to

record and transmit what goes on inside of our bodies to a remarkable extent. Rather than be fearful of these advances, he encouraged the Committee to look beyond the question of data sharing and instead, consider ways to control its use, its security, and access. Much of our current regulatory regimes simply don't work for this massive data flux. The idea of notice and consent and expecting consumers to read and understand complicated terms of use and agreement are unrealistic and ineffective.

He explained how companies related to the healthcare industry are relying on algorithms to decide who gets what kind of information and that kind of access is becoming increasingly more important.

He recommends that regulations be put into place for companies to understand the implications and extent of this practice, the kind of data involved in these algorithms as well as repercussions. Also important is appreciating the results and outcomes of the calculations. Setting up programs or developing policy by formula may impact certain groups while some populations may be inadvertently excluded resulting in uneven treatment and even discrimination. He noted that there should be sensitivity that data capturing aspects of social class, economic status and geographic settings can impact and skew results and further compromise populations.

Kevin Stine, Chief Applied Cybersecurity Division, National Institute of Standards and Technology's Information Technology Laboratory

Mr. Stine provided an overview of his agency's mission -- to cultivate trust in information and in systems. One component is to help organizations understand and manage cybersecurity risk. They accomplish that through a combination of research and development and application of standards, guides, best practices, tools, reference resources, and measures. A central point is the National Cybersecurity Center of Excellence whose purpose is to accelerate the adoption of secure technologies by collaborating with industry to use best practices and commercially available technologies to help solve business and cybersecurity challenges.

Mr. Stine then reported that NIST anticipates developing and issuing guidelines for the "Internet of Things" including cybersecurity and privacy considerations for federal agencies this year. He noted how organizations are developing best practices to secure connected devices and technologies in the healthcare space.

Adam Greene, Partner, Davis Wright Tremaine

As part of his introduction, Mr. Greene shared that prior to joining the law firm, he worked at HHS on HIPAA projects first at the Office of General Counsel and then with the Office for Civil Rights.

Mr. Greene described how regulations and legislation overlap to the extent that in some cases, just because HIPAA may not apply, that does not automatically mean that the information is unprotected under law. For example, the data may be subject to the FTC Act, the Safe Medical Record laws, or state consumer protection laws. The most significant challenge is that these laws are poorly communicated and misunderstood, thus limiting the guidance and effectiveness.

At the same time, there are loop holes in HIPAA protections. Mr. Greene provided an example of a "HIPAA hot potato," when the same information can jump from being subject to HIPAA and then depending on access and use, can fall outside of HIPAA (example: claims information available to members through the Blue Button initiative). It is difficult enough for providers, plans, and app developers to understand where HIPAA does and does not apply in situations, let alone the average consumer to fully understand these details.

In order to assure consistency, he recommends national uniformity where states and federal agencies should strive for uniformity in their privacy and security laws. With so many rules poorly understood and explained, providers and stakeholders stay stuck in ineffective and inefficient practices. He concluded that uncertainty stifles innovation. Entities that are not subject to HIPAA are often involved with exciting, cutting edge innovation. What's needed are clear, uniform, reasonable, and readily achievable requirements to level the playing field to encourage innovation.

As challenging as it can be to comply with HIPAA, complying with the ambiguity of the other laws can be even more of a challenge. The answer is not that more privacy and security laws necessarily equal better protection. Instead, everyone who has a stake in governing health information must better coordinate to provide regulated entities with uniform, understandable, and actionable steps to address privacy and security.

Discussion

When asked about the numerous options and requirements to meet privacy standards, the presenters noted that having a framework is a way to align and harmonize various requirements or expectations for meaningful impact and interaction. NIST's National Cybersecurity Framework was cited as an example, as well as vendor management. Presenters also noted the importance of improved coordination between groups as well as communication. Mr. Greene explained, "Yes, there are different laws, but let's try to interpret them uniformly." More clarity in communication would distinguish between what would be considered best practice versus what is actually legally required in legislation. He also suggested a move towards more actionable items, very clearly delineated requirements and expectations.

Several agreed that conflicting requirements across federal and state complicate matters, and sometimes, there is no law at all. They agreed that problems with anonymization and reidentification, persist and some wondered about the feasibility of an analytic framework to address. They also agreed on the need for more uniform tools for risk assessment to counter the current subjective analyses subject to different interpretations. Having basic minimums in terms of understanding would improve not only security, but also privacy and data governance.

The presenters also agreed that there are serious privacy and security concerns around identifiable data. At the same time, Mr. Greene specifically cited regulation 42 CFR Part 2, the law governing alcohol and drug abuse treatment records as an example arguably of what not to do on this front. As interpreted, the regulation locks down the information so tightly to be essentially unusable. One

suggestion is instead of focusing on how to limit the information, the objective should be making sure the data are not used in a way that will negatively impact the patient.

In response to a Committee member's question about how to even define health data, achievable rules and regulations, and mitigating actual risk, presenters commented on the enormity of the system involving data use and essentially agreed—"the more that we can have uniform tools available and agreed upon to assess risk, the better."

The participants also commented on distinctions between "controlling" "sharing" and "use" in terms of data collection, noting the enormous impact of personal devices in this expanding realm. Mr. Borden concluded that the objective should be to strive for societal benefit by the sharing of information while protecting the individual. Mr. Greene referred to the current opioid epidemic as an example of health providers trying to coordinate care and effectively manage treatment while stymied by "decades old statues and laws that essentially preclude robust sharing of information for good purposes like care coordination because of the fear of its misuse for very specific purposes."

A Committee member's question about health literacy sparked discussion about patient control over their data, including a suggestion to remove control of the data out of the hands of the data subject. The presenters expressed concern about the extent of interest and/or knowledge that consumers are expected to have in analyzing impossibly complex materials. With the ways and extent that data get transferred, patients/consumers can be baffled trying to determine who has what information, which can lead to misinformation. A "usability standpoint" might help clarify the extent of data utility.

Ms. Francis expressed concern about research for non-academic purposes. In some cases, pharmaceutical companies conducting their own studies don't go through the academic rigors that medical centers are required to complete, submitting to IRBs for clinical trials, for example. Companies can conduct drug trials with private physicians, who supplement their income with payments they receive for entering patients into either stage three or potentially stage four post-marketing studies. She expressed concerns that the interest of these commercial IRBs are perhaps affecting the stringency and potency of the research being conducted, even though they are supposedly in compliance with the Common Rule.

The Subcommittee expressed appreciation to the presenters. The agenda then proceeded to review and discussion of the workplan. They discussed the time schedule by upcoming quarter and work product expectations including: preliminary 2018 plans to coordinate with staff at the NIH/National Library of Medicine for a presentation on UMLS, a hearing on Health Terminology and Vocabulary and the Environmental Scan being conducted for the Subcommittee.

There being no public comment, the meeting was adjourned.

To the best of my knowledge, the foregoing summary of minutes is accurate and complete.

/s/

Linda Kloss, Chair
Privacy, Confidentiality & Security Subcommittee
DATE: 11/29/17