Prepared Statement from Adam Greene
Partner, Davis Wright Tremaine LLP
to the National Committee on Vital & Health Statistics; Subcommittee on Privacy, Confidentiality, & Security

Health Information Privacy and Security Beyond HIPAA
Tuesday, November 28, 2017

Good morning and thank you for this opportunity to provide testimony to the Subcommittee on health information privacy and security beyond HIPAA. My name is Adam Greene, and I am a partner in the law firm of Davis Wright Tremaine and co-chair of its health information practice. My practice generally focuses on health information privacy and security, and in particular HIPAA. My clients include health care providers, health plans, and a wide range of business associates. Prior to joining DWT, I was with the U.S. Department of Health and Human Services for five years working on HIPAA-related issues, first within the Office of General Counsel and later within the Office for Civil Rights.

We all see HIPAA frequently misspelled with two "Ps" and one "A." It also is common to see the name of the statute misstated. The "Health Information Privacy and Protection Act," for example. But, if the "P" did in fact stand for "Privacy," we likely would have a very different statute. Congress likely would not have enacted a health information privacy statute that was limited to a few specific types of "covered entities," and did not even cover all health care providers, let alone all holders of health information.

We are left with what I call "HIPAA Hot Potato." The same information can jump from being subject to, and then outside of, HIPAA. For example, a health care provider electronically submits a health care claim to a health plan. The information is subject to HIPAA while at the health care provider, the health plan, and any health care clearinghouse in between. The health plan then makes claims information available to members through the Blue Button initiative, resulting in a member using a personal health record app to download a copy of all of the member's claims information to the PHR's cloud-based application. At this point, the information that the PHR vendor maintains on the member's behalf is no longer subject to HIPAA. Then the plan member goes to a physician and instructs that the physician can securely receive a copy of the plan member's claims data – a wealth of information – if the physician downloads a version of the PHR software. The physician does so, and securely receives a copy of the claims data. The information is now subject to HIPAA again, as the vendor is now maintaining a copy of the claims data on the physician's behalf. It is difficult for providers, plans, and app developers to understand where HIPAA does and does not apply. We cannot expect the average consumer to do so.

Just because HIPAA does not apply, though, does not mean that the information is unprotected under law. Information that HIPAA does not govern may be subject to the FTC Act, to state medical records laws, or to state consumer protection laws. The most significant challenge is that these laws usually offer little guidance in the area of information security, and may even include conflicting requirements.

In considering how to best address health information privacy and security beyond HIPAA, I recommend considering a few general principles:

1. **HIPAA Is Not a One-Size-Fits-All Solution.** HIPAA was drafted specifically for health care providers and health plans. It is not necessarily a good fit for other types of entities. We already see this with requirements like the Security Rule's requirement to put in place an emergency mode operation plan, for example. Such a concept may make a lot of sense for a hospital that needs to provide critical patient care during a disaster, during which it may be operating off of a generator. It does not make as much sense for a business associate that is doing data analytics for a health plan. Extending HIPAA to more and more entities, which often have little in common with a hospital, for example, will lead to a lot of unnecessary administrative burden and confusion, without corresponding benefit.

2. **Uncertainty Stifles Innovation.** Entities that are not subject to HIPAA are often involved with exciting, cutting-edge innovation. Frequently, they are start-ups with very limited resources. It is challenging for them to comply with laws that merely require "reasonable" information security, without any details as to what is considered reasonable. What are needed are clear, uniform, reasonable, and readily-achievable requirements. Because technology is constantly changing, these requirements should be technology neutral or include readily-achievable minimum technology requirements (such as widely-available forms of encryption). Organizations generally want to provide good information security to customer health data, but need clarity regarding what they must do.

3. **National Uniformity.** Many of the most promising entities in the health care space do not have the resources to regularly conduct and update a 50-state legal survey on privacy and security laws, or stay informed of each new FTC settlement. California requires consents for health information to be in 14-point font. Texas requires consents to address electronic disclosure and to include special notice requirements. Massachusetts has its own detailed information security law for certain personal information. Navigating different consent requirements and different information security requirements takes valuable resources away from serving consumers and improving the health care system. Accordingly, states and federal agencies, such as the FTC, should strive for uniformity in their privacy and security laws. While this can be accomplished through federal preemption, it also can be accomplished through state governments cooperating on model laws. Consideration should also be given to the European Union's General Data Protection Regulation ("GDPR"), as more and more entities are striving to offer solutions internationally and seeking to create privacy and security programs that comply with both U.S. and E.U. law.

It is easy to fall victim to "HIPAA blinders," believing that HIPAA is the only law to worry about in health information. But, in fact, there are a number of laws that apply to health information beyond HIPAA. And 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. Rather, the answer is that 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.

Thank you for your time today.