Testimony of Sean P. Kelly, MD
Chief Medical Officer
Imprivata

Testifying before ONC's API Taskforce
January 28, 2016

I would like to thank the Taskforce for providing Imprivata with the opportunity to testify before the Taskforce. Imprivata is a healthcare IT security company that provides authentication, access management, and patient identification solutions. Our mission is to enhance the healthcare experience by making security convenient, streamlining the provider authentication process. Based in Lexington, Massachusetts, we come before the taskforce to provide insight into the evolving API industry.

I serve as the Chief Medical Officer for Imprivata, but also continue my work as an Emergency Physician. It's through that lens that I would like to speak to the Taskforce today. As an Emergency Physician, I strongly advocate for open frameworks that improve interoperability and access to patient data. Medically, ethically and legally, access to data has a significant impact on care delivery. For example, if I'm on call at 2 o'clock in the morning and a comatose patient presents to the ED, it is essential for me to access their protected health information, quickly and securely. Here are just a few of the questions I need answered upon arrival:

- What is the patient's medical history?
- Do they have a seizure disorder?
- Are they diabetic?
- Do they or their family have a history of heart disease?
- Is there any recent trauma?
- Is the patient on anticoagulants?
- What other medications do they take that could contribute to the differential or affect treatment?
- What is their code status? Do they have advanced directives and a healthcare proxy?

Each of these questions affects how I am going to administer care. Each of these answers should be available to me. It's not an exaggeration to say that having immediate access to pertinent data can be life-saving and directly affects patient safety and outcomes of care.

Our current system is broken. The fragmented databases storing patient information have become detrimental to delivering efficient and high quality care. In the current system, if a patient is followed at another hospital that uses a different electronic health record, I often cannot get access to that information in a timely manner, even when that hospital also happens to be affiliated with the same medical school as the one in which I work. These are not isolated or rare instances, but rather represent the norm that doctors, nurses, patients and family members are forced to deal with as the status quo.

I would strongly advocate for enforcing standards of integration that promote an open framework with architecture that allows for secure access to patient information. This type of system may require supervised enrollment, credentialing, and access controls using strong authentication methods. Despite these steps, a system of this complexity is preferable to not being able to access patient data when we need it most. And good technology can actually reduce the complexity of such security and privacy

standards, allowing for convenience and efficiency if implemented properly. This type of architecture already exists in many other industries in which privacy and security are of utmost importance. For example, in the financial sector, APIs and other mechanisms are used to ensure interoperability between institutions and customers in a secure and transparent fashion. From my understanding, the mortgage application process allows for participants to easily check credit scores and financial metrics. APIs in this sector also allow a consumer to give permission to financial institutions to perform the same functions on their behalf including checking various financial records and verifying eligibility for a loan.

I would not recommend ignoring the risks involved in streamlining access to patient records; however, there are effective ways to mitigate these risks. The precedent has been set within the healthcare industry for such a system. For example, the method of electronic prescription of controlled substances demonstrates how supervised enrollment procedures use strong authentication to comply with the strictest security standards in healthcare, set by the DEA.

In short, there are already proven methods in the healthcare industry and beyond that facilitate the secure exchange of potentially life-saving data while mitigating the risks of sharing that data. The risks of such interoperability are far outweighed by the risks inherent in **not** sharing essential data between caregivers. Lack of data interoperability is adversely affecting patients to a significant degree across the country on a daily basis. Most healthcare professionals would support a standardized architecture allowing for exchange of data, even if it required enrollment ahead of time and strong authentication methods, such as biometrics. I did it to get my Global Entry card... I would certainly do it to help my patients and comply with the Hippocratic Oath: "First, do no harm."

Thank you for inviting me to testify today.