TEXT OF TESTIMONY BY ROBERT STAUSS, FOUNDER AND CEO OF V26 LABS, TO THE DEPARTMENT OF HEALTH AND HUMAN SERVICES AND THE OFFICE OF MANAGEMENT AND BUDGET, NEW EXECUTIVE OFFICE BUILDING, WHITE HOUSE COMPLEX.

20 FEBRUARY 2020

21st Century Cures Act: Interoperability, Information Blocking, and. The ONC Health IT Certification Program

Good afternoon. Thank you for the opportunity to be here today, and to present my position on this critical issue.

First, I would like to briefly introduce myself. My name is Robert Stauss. I am an ethical hacker by background and training, and I have devoted my professional career to healthcare cyber and information security. Today I am the founder and CEO of v26 Labs, a healthcare information security company.

We are a company that is in business to protect healthcare organizations from getting hacked, and to protect the data of those healthcare organizations and, by extension, the millions of patients who receive their healthcare from those organizations. I want to emphasize that we are not a software developer. We do not develop software applications, nor do we develop APIs. The only code that we write are scripts that are used for security testing. We do not sell, publish or share our code.

I would like to make it known for the record that, as a whole, I support this Rule. Giving patients free and easier access to their data is a good thing, and it is something that I strongly support and encourage. With exception, I think that this proposed Rule is good, and I support its implementation.

It's the exception that brings me here today. That exception is in the area of the protection of data and patient privacy.

Under the Rule as proposed, many third-party companies that develop software and APIs will not be HIPAA compliant. This leaves data in the hands of developers who have nearly unrestricted collection and use of protected health information. Most of these companies are good actors, but some are not. More than that, this data will be in the hands of companies which generate a significant source of their revenue by selling data, or sharing data with third parties. The result of this is that patients who don't understand what they are signing up for when they accept terms of service agreements, and that is most of them, will have their protected health information out there and will have no control over what happens to it, or who views it.

I would like to give a few brief examples. Adolescents, who have had the benefit of having their protected health information restricted under the laws of many states, will find that information they reveal to their healthcare provider in confidence can and will likely be collected and used for purposes that no one can completely foresee. A possible scenario is we will likely see an app selling information to the parents of an adolescent patient.

Think about a 16-year-old patient within a strict household who was diagnosed with a sexually transmitted infection, and is currently being treated. With health data that is not sufficiently protected, that patient's parents or guardian can get a hold of that data and use it to punish that individual. Perhaps with that experience, that individual will no longer feel confident in confiding with his healthcare provider and will leave future medical issues undisclosed and therefore untreated.

Consider a 71-year-old patient who has a genetic syndrome that predisposes that individual to certain types of cancer. This individual has made the difficult choice to keep this information to herself for admirable reasons, which should be her right. Without privacy protections, software can link health records, and a family member will be able to see a family history that can be attributed to a specific family member. Now that individual's health information, which should have remained confidential, is out in the open.

The concern is not just limited to an individual's access to protected health information. We previously looked at the collection of data received by the health apps on a well-known smart watch. What was revealed was that when people were engaged in having relations, this activity was being collected by the smart watches. The question then is who can access this information? It turns out that the smart watches are not only collecting the data that you're engaged in having relations, but how often and, because of geolocation functionality, *where* you're having relations. The data is is then extracted by, among others, insurance companies who may then use the data to raise a customer's insurance premiums based on increased risk due to perceived promiscuity.

Finally, I would like to share an example of how persons within the vulnerable population can be victimized by the access of health information. I recently heard about a bad actor who was shown to successfully gain access to healthcare records and use that access to identify people with dementia and other cognitive disabilities. That bad actor then used that information to scam those victims out of their life savings.

These are just a few of many important examples to illustrate the importance of protecting health information.

If this Rule is implement before privacy protections, such as HIPAA compliance, are in place to protect health data, we will see more events of health data being used for sinister purposes and there is no turning back. For everyone in this room today, I would like you to think of some of the most private conversations that have taken place between you and your healthcare providers. Would you feel comfortable if I were to access it right now? Once data is out there, even if protections are put in place

later, the patient can never get that information back. It's out there forever. Patients need to have their clinical data protected.

If we lose the protected part of protected health information, it simply becomes information — and information to be shared freely between any number of software developers, individuals, media companies and insurance companies, just to name a few.

We have a responsibility to protect patients from the harvesting of their most sensitive information, and we must make sure that privacy protections, such as HIPAA compliance, and put in place before this Rule is implemented.

I have come here today independent of any other company, and without a political bias, to present my position and that of v26 Labs on this important issue. I am proud to lead this growing company, and I take very seriously the trust that is placed in us by our clients, and all of the patients whose data we work hard to protect. This is a critical moment in history, and I am honored to be able to share my viewpoint here today. Thank you for the opportunity, and I look forward to answering your questions.

- -