

May 18, 2016

**Via E-Mail (iotrfc2016@ntia.doc.gov)**

Mr. Travis Hall  
National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Room 4725  
Attn: IOT RPC 2016  
Washington, DC 20230

***Re: File Code: IOT RPC 2016 – Comments on The Benefits, Challenges, and Potential Role for the Government in Fostering the Advancement of the Internet of Things (“IoT”)***

Dear Mr. Hall:

I am responding to the Request for Public Comment dated April 6, 2016<sup>1</sup> on the Internet of Things, specifically to the following questions as they relate to IoT in healthcare:

3. With respect to current or planned laws, regulations, and/or policies that apply to IoT:

a. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?

b. Are there examples that, in your view, unnecessarily inhibit IoT development and deployment.

**Response – Need New Anti-Kickback Safe Harbor for IoT:**

By 2025, the total global worth of IoT technology could be as much as \$6.2 trillion, with roughly 40% of that value from devices in healthcare (\$2.5 trillion).<sup>2</sup> IoT value in healthcare will greatly benefit patients, the Government and the taxpayers by increasing healthcare quality and reducing healthcare costs.

<sup>1</sup> 81 Fed. Reg. 19956-19960 (Apr. 6, 2016).

<sup>2</sup> <http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html> (last viewed May 18, 2016).

Mr. Travis Hall  
National Telecommunications and Information Administration  
U.S. Department of Commerce  
May 18, 2016  
Page 2

The federal anti-kickback law<sup>3</sup> and the federal physician self-referral law (known as the “Stark Law”)<sup>4</sup> stand as major barriers to the realization of IoT benefits in healthcare. In 2004, the Centers for Medicare and Medicaid Services (“CMS”) created a regulatory exception to the Stark Law for community-wide information systems<sup>5</sup> that is an example of an existing regulation that might be helpful in fostering IoT development and deployment in healthcare. However, the Stark exception for community-wide information systems has not been useful to date because there is no corresponding anti-kickback safe harbor for community-wide information systems. In order to foster IoT development and deployment in healthcare, the Government should adopt a new anti-kickback safe harbor for community-wide information systems that corresponds to the existing Stark exception.<sup>6</sup>

### **Simplify the Existing Stark Exception for Community-Wide Information Systems**

The existing Stark exception for community-wide information system is fairly straightforward, with only three conditions for the exception to apply:

1. The information technology items and services are available as necessary to enable the physician to participate in the community-wide health information system, are principally used by the physician as part of that system, and are not provided in a manner that takes account of referrals or other business generated by the physician;
2. The community-wide health information system is available to all providers, practitioners and residents in the community who desire to participate; and
3. The arrangement does not violate the anti-kickback statute or any billing or claims submission laws or regulations.

IoT includes information technology items and services that enable the physician to participate in information systems. The Stark exception requires that the information system be “community-wide” and “available to all providers, practitioners and residents in the community who desire to participate.” These requirements conflict with the common concerns in healthcare

---

<sup>3</sup> 42 U.S.C. §1320a-7b(b) (2016).

<sup>4</sup> 42 U.S.C. §1395nn (2016).

<sup>5</sup> 42 C.F.R. § 411.357(u) (2016); adopted at 69 Fed. Reg. 16054, 16112-16113 (March 26, 2004).

<sup>6</sup> Section 205 of the Health Insurance Portability and Accountability Act of 1996 requires the Government to annually solicit recommendations for developing new anti-kickback safe harbors, although the comment period for the most recent annual solicitation has closed. 80 Fed. Reg. 79803 (Dec. 23, 2015).

Mr. Travis Hall  
National Telecommunications and Information Administration  
U.S. Department of Commerce  
May 18, 2016  
Page 3

over privacy and security of individually identifiable healthcare information. The Stark exception also requires that the information technology items and services “are principally used by the physician,” which excludes IoT devices principally used by patients themselves, physician extenders or other non-human things. The third condition about not violating the anti-kickback statute is problematic until a corresponding anti-kickback safe harbor is created. The Stark exception would be even more useful for IoT if it was further simplified to only one condition:

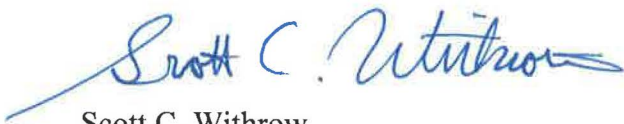
1. The information technology items and services are available as necessary to enable the physician to participate in a health information system, and are not provided in a manner that takes account of referrals or other business generated by the physician.

### **Conclusion**

I recommend simplifying the existing Stark exception for community-wide information systems as suggested above, and then adopting a new corresponding anti-kickback safe harbor. These simple steps would remove major barriers to the realization of trillions of dollars in value from IoT in healthcare.

I appreciate your consideration of these comments. Please feel free to contact me if I can provide any additional information.

Sincerely,



Scott C. Withrow