August 15, 2016

The Honorable Lamar Alexander
Chairman
Committee on Health, Education, Labor, and Pensions
United States Senate
Washington, D.C. 20510

Dear Senator Alexander:

I am writing on behalf of HITRUST to highlight the need to overcome a regulatory obstacle, embedded within the Stark law, for health care entities seeking to donate or subsidize cyber security programs. As you know, the Stark Law ("Stark") governs physician self-referral for Medicare and Medicaid patients.[1] Under Stark, a physician is prohibited from making a referral to an entity for the furnishing of designated health services ("DHS") payable by Medicare if the physician or an immediate family members of the physician has a financial relationship with the entity, unless a regulatory exception to Stark applies.[2]

Although Stark serves as a stringent barrier against fraud and abuse amongst health care providers, the law often proves inflexible in the context of rapidly advancing health care technology. Donating cyber security products and services to a physician is not to the benefit of one healthcare organization, but protects the wider health care ecosystem from cyber security breaches. However, cyber security transactions between providers inevitably trigger violations under Stark. As it stands, the law classifies a donation or subsidization of technology between a health care entity and another healthcare provider as a prohibited financial relationship.

While there is not a perfect solution to cybersecurity, the best strategy is to prevent, detect, and respond before the adversary achieves their objective. A data breach in the healthcare industry has dramatic consequences for patients, their families and inflicts financial and reputational harm on the company targeted by the threat actors. Beyond the privacy implications of data breach incidents, these breaches have the potential to, and have often disrupted the operations of a healthcare facility which can affect patient care. These complexities, interdependencies, and unique attributes create various risk levels that need to be considered across the continuum of care.

Empowering physicians to better manage their cybersecurity posture is key to minimizing the likelihood of a cyber related breach. We seek to eliminate regulatory barriers that make it difficult for physicians to actively engage in their cyber risk management.

The recent example of the Electronic Health Records ("EHR") exception[3] to Stark illustrates the positive effect of regulatory relief for health care providers. Until this exception was enacted, new information systems were often fiscally out of reach for many small physician practices. In an effort to address the issue and streamline physician/hospital alignment, health entities began to offer to donate or charge a significantly reduced rate for use of their EHR technology. Stark's classification of donated technology as a prohibited referral sparked industry wide frustration and prompted regulatory authorities to reevaluate the provision to incorporate these practical innovations.[4]

---

[1] http://starklaw.org/
[2] 42 U.S.C. §1395nn(a)(1); 42 C.F.R. §411.353(a)
[3] 42 C.F.R. §411.357(w)
[4] 71 Fed. Reg. 45140 (August 8, 2006).

While the Stark EHR exception bridges a crucial gap in health information sharing, and donating entities, receiving physician groups often lack adequate security systems to protect protected health information from cyber-attack. Small, ill equipped practices are vulnerable to security breaches which can ultimately infiltrate the larger healthcare environment through the exchange of patient data. Physician groups confront financial challenges in their ability to provide sufficient cyber security programs to protect their patient records, as this software service support is often expensive and difficult to manage without trained technicians. Again, we need to empower physician practices to actively manage their security posture, not hinder them.

Healthcare remains an ever growing industry and perhaps the most at risk area of critical infrastructure. The impact of a breach is felt industry wide and, given healthcare's unique qualities, often has a direct impact on the lives of individual patients. In order to accommodate crucial cyber security options for all health care providers, Stark requires amendment.

Similar to the method of incorporating EHRs, we propose an amendment to reflect an exception to Stark for the donation or subsidization of cyber security software. The Stark EHR exception[5] effectively addresses management of technology between health care entities and serves as a perfect template for an analogous cyber security provision. A new provision, **42 C.F.R. §411.357(x) Cyber Security Items and Services**, will mirror the wording of **42 C.F.R. §411.357(w) Electronic Health Records Items and Services** to a large extent and will provide a necessary protection for health care entities electing to donate or subsidize cyber security software service and support to other organizations.

We sincerely appreciate your consideration of our efforts to encourage the sharing of cyber information while providing vital cyber protection for health care providers.

Thank you,

Very truly yours,

Daniel Nutkis
Chief Executive Officer

CC:
The Honorable Patty Murray
Ranking Member
Committee on Health, Education, Labor, and Pension
United States Senate
Washington, D.C. 20515

[5] 42 C.F.R. §411.357(w).