ASCRS

AMERICAN SOCIETY OF CATARACT AND REFRACTIVE SURGERY

May 31, 2018

The Hon. Greg Walden
Chairman
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20515

The Hon. Frank Pallone
Ranking Member
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20515

Re: Supported Lifetimes Request for Information

Dear Chairman Walden and Ranking Member Pallone:

The American Society of Cataract and Refractive Surgery (ASCRS) is a medical specialty society representing nearly 9,000 ophthalmologists in the United States and abroad who share a particular interest in cataract and refractive surgical care.

We appreciate this opportunity to provide comments in response to the supported lifetimes request for information. The practice of ophthalmology relies heavily on the use of medical devices to diagnose and treat ocular diseases. Ophthalmology practices have been the victims of—and continue to remain vulnerable to—security breaches and cybercrimes due to outdated or unsupported operating systems and lax security protocols by medical device manufacturers. Ophthalmology practices tend to be small or solo practices unaffiliated with large hospital or health systems. As such, they may not employ full-time information technology (IT) professionals, and lack the technical expertise and resources to identify and correct potential vulnerabilities, or respond to and recover from breaches.

As the committee continues its investigations and policy development related to healthcare cybersecurity, we urge you to focus on several key issues:

- The impact of potential cybersecurity breaches on small and solo physician practices. Physicians should be focused on providing patient care and should not be solely responsible for ensuring the medical devices they use are adequately protected from cyberthreats.

- Ensuring medical device manufacturers provide adequate protection from cyberthreats to medical devices, especially those using outdated or legacy software.

- Ensuring that medical device manufacturers are aware of and do not create additional vulnerabilities through ongoing remote service for equipment.

Full information on these points is provided below.

Reducing the Burden of Cybersecurity on Small Practices

Physician practices are gathering and managing an increasingly large volume of patient healthcare data. Electronic health records (EHR) have become prime targets for cybercriminals seeking personal information that is not otherwise available, and physician practices are liable for any breaches of patient data that result from cyberattacks. As physicians, ophthalmologists take their responsibility to guard patient privacy seriously, and must ensure that all entities they work with also take that duty seriously. However, since they typically practice in small or solo independent groups, ophthalmologists often lack the resources to protect electronic data adequately if there are vulnerabilities in their medical devices. ASCRS recommends the E&C Committee explore ways to assist small practices in preventing and responding to cyberattacks through outdated or unsupported medical device software, such as requiring medical device manufacturers to communicate to practices when software is out of date or unsupported, or if there are known vulnerabilities in the device's operating software.

- **Ophthalmologists tend to practice in small or solo groups that may not have the resources to identify and respond to potential cyberbreaches from medical devices.** A recent survey of ASCRS' membership found that 76% of our members practice in groups of 10 or fewer physicians, with 15% reporting they are solo practitioners. While many of these small practices may use cutting-edge technology to diagnose and treat patients or use EHR systems to track patient care and communicate with patients and other practitioners, they may not have the resources to employ full-time IT staff, especially those with cybersecurity expertise.

- **Ophthalmology practices rely heavily on medical devices to diagnose and treat ocular disease, making them particularly vulnerable to cyberattacks.** A typical ophthalmology practice may use several different medical devices on a regular basis in their practice, such as biometric measuring devices, ultrasound equipment, fundus cameras, topographical measuring devices, visual field equipment, ocular surface disease treating devices, autorefractors, and autokeratometers—to name a few. Nearly all of these devices are run by software systems and may be connected to the practice's overall network. As the RFI notes, these highly specialized devices often cost the practices hundreds of thousands of dollars and cannot be quickly or easily replaced if potential software vulnerabilities are identified, especially if they are still functioning well for the intended purposes of diagnosis or treatment. Given the wide array of medical devices used by a typical ophthalmology practice, they may have several different devices that may use different operating software in varying states of readiness to protect against cyberthreats.

- **Ophthalmology practices may not have the staff or resources to adequately identify all potential vulnerabilities in their medical devices.** Physicians have a legal and ethical duty to protect patient data, and ophthalmology practices have implemented protocols in their practices to ensure systems, such as EHRs and practice management, are secure. These practices may be less equipped, however, to deal with potential breaches from medical devices. While some ophthalmology practices may employ full-time IT professionals, many do not, and without specialized knowledge of a particular device's software, even full-time IT staff may not be able to understand and protect against potential breaches through outdated or unsupported software.

- **Physicians and practices should focus primarily on patient care rather than cybersecurity.** As mentioned above, physicians do take their duty to protect patient data seriously; however, as medical professionals, they cannot be expected to be security experts as well. A busy ophthalmology practice offering surgical treatments for ocular disease, such as cataracts, and care for sight-threatening chronic diseases, including glaucoma, corneal disease, and macular degeneration, relies on many different medical devices to help diagnose and treat patients. Physicians should be responsible consumers who do their due diligence to ensure the medical device manufacturers they are purchasing from are aware of and addressing potential vulnerabilities, but the ultimate responsibility for ensuring the long-term cybersecurity of the device rests with the manufacturers. They are uniquely positioned to understand how the systems their devices use may be impacted by threats, and how to respond when breaches do occur. **Physicians should be vigilant against potential cyberthreats but focus their primary attention on taking care of patients.**

Ensuring Protection from Cyberthreats Due to Outdated Software

Medical device manufacturers have a duty to ensure that physicians who use their devices are aware of potential vulnerabilities in their systems due to outdated and unsupported software programs. The Committee's RFI notes that requiring medical device manufacturers to keep all software programs up to date and supported would likely be unworkable, especially on equipment that has also reached the end of its useful life for treating or diagnosing disease. However, given that small medical practices that use these devices may not have the resources or technical expertise to identify and respond to potential vulnerabilities from outdated or unsupported software, it is incumbent upon the manufacturer to inform physicians and practices when they determine that the software can no longer be supported or updated. Practices need to be aware of the potential liability for cyberbreaches of patient data they are incurring due to unsupported software systems.

- **We recommend Congress seek solutions for ensuring medical device manufacturers adequately communicate to their customers the risks associated with unsupported software.**

Ensuring Ongoing Medical Device Cybersecurity

While ASCRS believes that medical device manufacturers should be required to inform physicians and practices when software is out of date or unsupported, we believe the Committee should take a wider look at medical device cybersecurity and address potential vulnerabilities not related to unsupported software, such as networking and remote service and monitoring.

- **Many of today's cutting-edge medical devices, especially in ophthalmology, are designed to interface with other technology in the practice to deliver seamless and instant information to physicians.** Ophthalmology practices may be using several different devices that are integrated with their EHR or practice management systems to facilitate image viewing, documentation, coding, and billing. These technical advances can greatly improve a physician's efficiency by organizing test results, images, and a patient's history into one place. However, as physician practices become increasingly networked, their cybersecurity risks increase as well.

- **Without proper security for networked medical devices, those devices can pose a threat to the practice's overall cybersecurity.** Physicians and practices are aware of the threats to patient data and take steps to protect IT systems that deal with that data directly, such as EHRs and practice management software. However, they may not be aware of, or have any way to detect, potential vulnerabilities in software that operates their medical devices.

- **Devices connected to a practice's network, and that feature remote monitoring from the manufacturer, are particularly vulnerable to cyberattacks.** For example, ASCRS heard recently from a solo ophthalmology practice in Connecticut that had several pieces of equipment from the same manufacturer, which are networked and integrated with the practice's EHR. As a result of a yearly security risk analysis conducted by an outside IT vendor, the practice became aware that there was an unsecure link back to the manufacturer that allowed it to perform routine services on the device remotely. The practice rectified the potential vulnerability by requesting the manufacturer disable the connection and only re-establish it when the device was in need of service or repair. While this practice was able to correct the issue before any breach occurred, it demonstrates that the practice was not aware of the potential vulnerability, and the manufacturer itself did not consider the potential risks in its system.

- **Device manufacturers must be required to provide information, both at the initial point of sale and throughout the device's life, about potential security vulnerabilities in their systems.** Physician practices do not have the ability to predict or detect what devices might have potential software security flaws. Device manufacturers know what software their products use and should be taking ongoing action to identify and protect against cyberthreats. When device manufacturers do encounter these vulnerabilities, they should warn practices about the potential for a breach, and take necessary action to fix them. **We encourage the committee to seek policy solutions that will ensure device manufacturers consider potential security risks in their systems and communicate them to practices using their equipment.**

Conclusion

Thank you again for the opportunity to provide information on the cybersecurity threats posed by medical devices. We ask that the committee take into account the risks and liability from potential breaches that practices, particularly small ophthalmology practices, are taking on from unsupported or out-of-date software on medical devices. In addition, we encourage the committee to investigate further the potential threats from unsecure networked devices. **We ask the committee to require that medical device manufacturers make practices who use their products aware of potential vulnerabilities in their devices—both from software that is no longer supported and software still in current use.**

If you have questions, please contact Allison Madson, manager of regulatory affairs, at amadson@ascrs.org or 703-591-2220.

Sincerely,

Thomas W. Samuelson MD

Thomas W. Samuelson, MD
President, ASCRS