Opening Statement of the Honorable Michael C. Burgess, M.D.
Subcommittee on Oversight and Investigations on
"Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity"
June 7, 2017

Good morning. Cybersecurity in the health care sector is a timely topic that has real, physical consequences. In almost three decades as a practicing physician, ransomware was never an issue I faced. Now, the threats posed by malicious actors are almost universal across the sector due to legacy systems, poor cyber hygiene, and a severe shortage of qualified cybersecurity professionals.

Most cyber attacks have the potential to cause real harm, depending on the severity and target. However, in health care cybersecurity, it is a certainty. Anytime information in the health care and public health sector is compromised, it poses a risk to providers, patients, and all those who serve and supply them.

The recent WannaCry ransomware infected thousands of computers across the world and severely impacted the health care sector in the United Kingdom. While the U.S. health sector was largely spared from this paralyzing malware, some organizations continue to deal with the effects of trying to eradicate this virus from their systems. The ease with which WannaCry was able to infect so many systems is alarming – and it was entirely preventable. While this particular malware only sought to lock information until a ransom was paid, the threshold remains low for more malicious actors to access critical health systems. We must work to acquire the cyber expertise, resources, and structure to combat such vulnerabilities.

The report produced by the Health Care Industry Cybersecurity task force is a step in the right direction in improving our ability to prevent and respond to cybersecurity

events. The report also identifies the challenges posed by the health care and public health sector in maintaining security across unique platforms and devices that must all work in concert to enable accurate and timely patient care.

This is even more important when considering that health information isn't something you can easily change, such as a credit card or phone number. Your health information is your information for life, and the integrity of this data is paramount to protecting patient safety. Can you imagine the consequences of altering a person's blood type, allergies, or disease diagnosis in a system relied up on by providers to treat patients?

Overall, the health care and public health sector has improved its ability to manage cybersecurity events, including HHS' management of the WannaCry malware that resulted in minimal effect on U.S. health organizations. But the balance between securing important data and protecting patient privacy

needs continuous evaluation and adjustment. Is there a point where information sharing creates more vulnerability by identifying entities as targets of attack? What happens when health care organizations limit reporting of breaches or the sharing of information for fear of losing customer confidence or becoming a target? How do we increase the availability of cybersecurity professionals in the health sector? I look forward to discussing these and other issues with the witnesses today. Thank you.