American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

February 27, 2020

The Honorable Rick Scott
United States Senate
B3 Russell Senate Office Building
Washington, DC 20510

The Honorable Marco Rubio
United States Senate
284 Russell Senate Office Building
Washington, DC 20510

The Honorable Tom Cotton
United States Senate
124 Russell Senate Office Building
Washington, DC 20510

Dear Senators Scott, Rubio and Cotton:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to respond to your questions on efforts to protect U.S. taxpayer-funded research developed at our member organizations from foreign threats.

Hospital and health system leaders recognize that the information and resources held by their health care organizations are highly sensitive and valuable, and they are taking both cyber and intellectual property (IP) security challenges extremely seriously. They have implemented important security steps to safeguard clinical technologies and information systems while continuing to enhance their data protection capabilities. Hospitals and health systems have made great strides to defend their networks, secure patient data, preserve the efficient delivery of health care services and, most importantly, protect patient safety.

The AHA has focused its efforts on providing up-to-date cybersecurity and risk information – for both technical and non-technical audiences – to our member hospitals and health systems. This information assists hospitals and health systems as they face the continuing challenges of ensuring the privacy and security of medical research and patients' health care data in an environment of increasingly networked technology and expanded connectivity that offers significant benefits for care delivery, but also increases the potential for exposure to additional security threats. Our detailed comments on specific areas follow.

AHA's Efforts to Address Foreign Threats

The AHA is acutely aware of foreign threats and influence to medical research and related IP and is actively working to help our member hospitals and health systems to mitigate those risks. The AHA began raising awareness of these issues in 2014 with resources directed at both hospital and health system leaders and trustees. In 2018, the AHA expanded its educational opportunities for members, providing targeted and customized information, including strategic cybersecurity and risk advisory services.

Specifically, the AHA created a new role, senior advisor for cybersecurity and risk, to assist the field. We hired a nationally recognized health care cybersecurity expert who has nearly 30 years of highly-accomplished service with the Federal Bureau of Investigation (FBI) to help raise member awareness of the general cyber threat landscape, as well as specific threats from adversarial nations including China, Russia, Iran and North Korea.

Through this new position, the AHA has been able to work closely with federal government partners to help increase the coordination and sharing of information to identify possible threats, such as China's prolific and aggressive campaign to obtain U.S. medical research and IP. The AHA serves as both a distribution channel to disseminate threat information, as well as a conduit to federal agencies and departments highlighting hospitals' and health systems' on-the-ground experiences. This unique partnership allows the AHA to create educational material on various threats, develop best practices and methodologies to identify, mitigate and disrupt threats, and facilitate the exchange of information.

Education is Needed to Prevent Additional Theft

The AHA offers many educational opportunities to hospital and health system leaders, including both in-person and web-based presentations discussing specific cyber and IP security topics. We have prioritized raising awareness for board members, hospital leaders and staff, in addition to providing information to technical audiences. The AHA reviews government policy, regulation and legislation to provide analysis on risk implications for hospitals and health systems. We monitor pending criminal and national security investigations and liaise with law enforcement and the intelligence community, as needed. The AHA also offers support and advice to members when incidents occur that affect their organizations.

A primary focus of our education efforts has been raising awareness of China's efforts to acquire medical research and IP through various legitimate business and research relationships and through illegitimate means, such as theft, diversion and compromise. The AHA has suggested methodologies to detect, deter and disrupt threats to medical research through a process that includes cataloguing research, risk classification and prioritization of research in terms of impact to public health and safety, national security, economic security and business risk. These processes combine a number of physical, personnel and

cybersecurity controls designed to protect medical research based upon risk stratification and prioritization. The AHA recommends the following steps to the field to mitigate the risk of IP theft:

- **Educate** – Create awareness and support among leadership, researchers and staff in an audience-sensitive manner of the foreign influence threats to medical research and innovation.
- **Catalogue** – Make an accurate accounting of all research and development activities, IP and other data, including where it is stored and who has access to it.
- **Classify** – Conduct a risk classification of identified and catalogued material to determine its value from a business and adversarial perspective and potential risk impact, including risk to public health and safety, national security and economic security.
- **Control** – Create security control tiers, or "risk stratification," around that research catalogue with the most valuable data requiring the highest level of security. It is essential to have controls that combine information security, personnel security and physical security.

We also recognize there is not a one-size-fits-all-method to protect against IP theft. Hospitals can and should approach threats differently based on their individual resources and circumstances surrounding their medical research and IP.

Throughout our member education efforts to minimize risks to research, the AHA has continually stressed the need to avoid even the perception of ethnic targeting or profiling. We advise members to distinguish between the activities of the Chinese government and the Chinese individuals who continue to make significant contributions to the advancement of science and medicine in the U.S. The AHA advises that investigations regarding theft of IP should be predicated upon improper behavior or illegal conduct and not race or ethnicity.

EFFORTS TO IMPROVE PROCESSES

As a membership association, the AHA focuses on providing members with the resources needed to protect their medical research. The AHA does not have the capability to track how each individual member organization implements or adheres to federal guidelines and requirements related to taxpayer funded research. However, our national awareness campaign has raised the profile of this issue, and we have received strong positive feedback from our member organizations. Many hospitals and health systems engaged in taxpayer-funded research now place special emphasis on requiring full and ongoing disclosure of potential conflicts of interest through review of federal research grant applications, organization non-disclosure agreements and data transfer agreements.

MORE FEDERAL INFORMATION SHARING AND ASSISTANCE IS NEEDED

The AHA continues to encourage members to engage with government agencies for resources and guidance on potential threats to medical research, controls to protect IP and processes to prevent conflicts of interest or illegal activity by researchers. The field is taking significant steps to protect taxpayer-funded research; however, current processes vary greatly.

The AHA appreciates the government's increased sharing of threat intelligence. These efforts, including coordinated declassification and release of threat information and targeted classified briefings, have been very helpful and they have greatly improved in the past several years. However, additional assistance from the government is needed to ensure all hospitals and health systems have the resources and information they need to identify high risk research programs and individuals within their organizations who may be improperly and secretly collaborating with foreign governments to illegally transfer research information out of the U.S. We recommend additional information sharing through the establishment of an interagency system that provides a regular cadence of classified and unclassified briefings for those who need to know that information to better prepare and protect organizations holding sensitive IP. This will greatly assist hospitals, health systems and academic medical centers to understand the nature of the external and internal threat they face and the foreign adversary's tactics to illegally transfer research information out of the U.S.

CONCLUSION

Hospitals and health systems are making important strides to defend medical research from foreign threats and any others. The AHA looks forward to continuing to work with government agencies and our member organizations to help decrease the vulnerability of the nation's IP.

Thank you for the opportunity to comment and for your leadership on this issue. Please contact me if you have questions or feel free to have a member of your team contact Aimee Kuhlman, senior associate director of federal relations, at akuhlman@aha.org or (202) 626-2291.

Sincerely,

/s/

Richard J. Pollack
President and Chief Executive Officer