HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

October 17, 2018

Don Rucker, M.D.
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Rucker:

As co-chairs of the Policy Task Group of the Healthcare and Public Health Sector Coordinating Council (HSCC) Cyber Security Working Group (CWG), composed of 198 healthcare organizations, companies and associations from across the healthcare industry, we are pleased to comment on behalf of the HSCC CWG members on the request for information (RFI) published in the *Federal Register* on August 24th on the Electronic Health Record (EHR) Reporting Program established under Section 4002 of the 21st Century Cures Act.

The organizations representing the Health and Public Healthcare Sector Coordinating Council's Joint Cybersecurity Working Group's (HPH JCWG) Policy Task Group span the health care sector and have a vested interest in advancing the cyber posture of the healthcare industry and improving patient safety. Our members are responsible in different capacities for protecting and securing patient information, something that is fundamental to spurring a healthcare system that is driven by value rather than volume. Given our focus on cybersecurity, our comments on the RFI will be limited the questions raised by ONC on this topic.

Need for greater cybersecurity focus

We urge ONC to focus on more transparency around electronic health record (EHR) vendors' cybersecurity posture. Given the growing cybersecurity threats to our sector, we recommend ONC recognize these challenges across all their programs and initiatives. As noted in the Healthcare Industry Cybersecurity Task Force Report published in June 2017, "The attack surface of the health information system expands when interconnected devices, such as mobile devices, medical devices, and applications, are permitted to connect to EHRs. Further complicating the health information system and EHR integration is the mobile device/application component. For simplicity, the EHR is the hub and connected medical devices are spokes." While our industry continues to mobilize and is working hard to catch up as a sector – and is making progress as outlined in a recent HSCC blog post.- we have traditionally lagged other critical infrastructures, The challenges to our sector are abundant and we believe these attacks pose direct threats to patient safety. In fact, in a report published October 5th by KLAS on medical device security a key finding that was patient safety is a top concern for providers.

Questions Posed by ONC

Q. What reporting criteria could provide information on meaningful differences between products in the ease and effectiveness that they enable end users to meet their security and privacy needs?

R. The following items would be helpful in better informing a purchaser of the vendors security posture:

1. Access to an auditor's statement regarding the security posture of the vendor and its products upon provider request.
2. Membership in an ISAO and ISAC.
3. Software Security Analysis.
4. If two-factor authentication is in use and what options are available for this.
5. Encrypted database features.
6. Information on role-based access control and how roles are configured.
7. Password protection policies (i.e. NIST standards).
8. Audit trails and reports configuration.
9. Patient consent opt-in agreement policies.
10. Custom privacy policy and terms of conditions for portals.
11. Payment Card Industry Data Security Standard compliance for credit card transactions.
12. Contractual clauses that prohibit providers from sharing of vulnerabilities with others (i.e. peers with the same EHR platform).
13. Policies on integrating mobile and biometrics.
14. For each release and upgrade, report the number of patches provided to address security related issues.

Q. Describe other useful security and privacy features or functions that a certified health IT product may offer beyond those required by HIPAA and the ONC Health IT Certification Program, such as functions related to requirements under 42 CFR Part 2.

R. Automated features associated with patient privacy would be very helpful and desirable for providers. Vendors should be able to track right of access, automate and track fulfilment requests such as when a patient has requested an amendment to their record. Also, automating patient preferences around restrictions associated with sharing records, as well as, accounting for disclosures. Managing any of these requests is a challenge for providers of any size thus knowing whether these features exists would provide utility for providers.

Q. Discuss the merits and risks of seeking a common set of measures for the purpose of real world testing that health IT developers could use to compare usability of systems.

R. A common set of measures a provider could assess against and measure to better gauge the security features of an EHR would be helpful. This should be considered a "floor" rather than a "ceiling" such that more vendors could exceed and even be encouraged to share more information.

Q. What information about a certified health IT product's security and privacy capabilities and performance have acquisition decision makers used to inform decisions about acquisitions, upgrades, or use to best support end users' needs?

R. More information about third parties used by EHR vendors would be helpful. For instance, are they contracting with third parties outside of the U.S. Often this information is missing in contracts and providers have little way of finding this information on their own. We also recommend that EHR vendors provide supportive documentation, like that created by the Office for Civil Rights (OCR) and ONC's risk assessment tool, to assist purchasers in their own risk assessments.

Q. What, if any, types of information reported by providers as part of their participation in HHS programs would be useful for the EHR Reporting Program (e.g., to inform health IT acquisition, upgrade, or customization decisions)?

R. Vendors sell upgrades in a variety of ways and there is no standard way for reporting vulnerabilities. Consideration should be given to having a more uniform way to do this, as well as, a record of patches required after releases and upgrades to address vulnerabilities be reported. Further, vendors could disclosure whether they are using the NIST Cybersecurity Framework as a means to address both standards and related compliance/disclosure.

Conclusion

The HSCC CWG appreciates the opportunity to comment on this important issue and urges ONC to factor into the EHR Reporting Program the growing incidences of cybersecurity attacks on our sector and the need to work collaboratively to address the threats.

Sincerely,

Carl Anderson, J.D.
Chief Legal Officer & SVP Government Affairs, HITRUST
Co-Chair, HPH SCC JCWG Policy Working Group

Theresa Meadows, MS, RN, CHCIO, FHIMSS
CIO
Cook Children's Health Care System
Co-Chair, HPH SCC JCWG Policy Working Group

Mari Savickis, MPA
VP, Federal Affairs, College of Healthcare Information Management Executives
Co-Chair, HPH SCC JCWG Policy Working Group