March 1, 2018

Seema Verma
Administrator
Centers for Medicare & Medicaid Services
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Administrator Verma:

The Association for Executives in Healthcare Information Security (AEHIS), is pleased to respond to the Center for Medicare & Medicaid Services' (CMS) call for improvement activities under the Medicare Incentive-based Program (MIPS). We are writing to recommend that CMS add an activity for which clinicians would receive credit for meeting cybersecurity best practices.

AEHIS represents more than 800 chief information security officers and provides education and networking for senior IT security leaders in healthcare. Below, please find our ideas for a safe harbor pertaining to donations involving cybersecurity.

As one of sixteen critical infrastructures, the healthcare sector is notoriously behind other sectors in its ability to fend off cyberattacks. Cyber threats are only growing more frequent and complex. With the increasingly interconnected nature of our healthcare system this poses a mounting risk to patient safety and clinicians are woefully unprepared to fend off these attacks.

Appended below are our submissions in the form of the template supplied by CMS. Please don't hesitate to contact our staff, Mari Savickis, vice president, federal affairs, at msavickis@chimecentral.org with any questions you may have.

Sincerely,

Erik Decker
Chair, AEHIS Board
CISO and Chief Privacy Officer
University of Chicago Medicine

Proposed Improvement Activities Recommended for Inclusion in the

Quality Payment Program: Submission Template

Cybersecurity Activity Submission	
Activity Sponsor: Provide entity name, URL, and individual contact information: name, address, phone, email—in case we need to contact submitter	Association for Executives in Healthcare Information Security (AEHIS) Mari Savickis, Vice President, Federal Affairs 20 F Street, NW 7th Floor Washington, DC 20001 Msavickis@chimecentral.org 202-294-3828 (c)
CMS NPI # or Sponsor Type: Include NPI number, or indicate other entity type, e.g. EHR vendor, specialty group, or other—25 words or less.	AEHIS represents more than 800 chief information security officers and provides education and networking for senior IT security leaders in healthcare. Below, please find our ideas for a safe harbor pertaining to donations involving cybersecurity.
Activity Title: Provide the activity title only—10 words or less	Meeting cybersecurity voluntary best practices.
Activity Description: Provide a brief description of the proposed activity—300 words or less. Please be as specific as possible about what the activity entails. E.g., "Eligible clinician must perform/do XXXX."	Meeting at least 75% of the best practices developed as part of Section 405(d) of the Cybersecurity Information Sharing Act of 2015 (CISA) should be considered for inclusion as an improvement activity. Under Section 405(d) of CISA the Secretary together with the National Institute of Standards & Technology (NIST) and the Department of Homeland Security (DSH) must establish best practices for meeting common, current day cybersecurity threats. A public / private workgroup has been working to establish these best practices which will be released in draft form and pilot tested in 2018. They are expected to be ready for use in 2019. The Health Care Industry's Cybersecurity Taskforce report, also mandated by CISA, was required to submit recommendations to Congress on ways to fortify the healthcare sector cybersecurity posture. The report was released in the summer of 2016 and work is underway to begin operationalizing the recommendations. Some recommendations are aimed at the public sector and some at the private sector. Recommendation 1.2 in their report called establishing "a consistent, consensus-based health care-specific Cybersecurity Framework." CMS has been involved in both the 405(d) and the Task Force work.

Validation of Activity: Supporting Website(s): Provide any supporting validation documentation that describes why the activity being proposed leads to quality improvement in the practice, improvement in patient health, experience, etc. AND/OR provide links to validated tools, processes referenced in the activity. (Please include URLs only	Cybersecurity Task Force Report - https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx - https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf Cybersecurity Information Sharing Act of 2015 (CISA) - https://www.gpo.gov/fdsys/pkg/PLAW-114publ113/pdf/PLAW-114publ113.pdf - (see starting page 696; page 741 discusses Section 405) ABC News Segment on cyber hacks of medical devices (simulated attack with clinicians) - https://www.youtube.com/watch?v=pU3NQ3GkC_0 Also see attached: - NEJM article Contacts on 405(d) Best Practices: - Julie Chua, HHS Security Risk Management Division Manager, Office of the Chief Information Officer (co-chair) - Erik Decker, Chief Security and Privacy Officer, The University of Chicago Medicine (co-chair) - Emery Csulak, CISO, CMS Contacts on Taskforce Report: - Emery Csulak, CISO, CMS (co-chair) - Theresa Meadows, CIO, Cook Children's Health Care System (co-chair) - Steve Curren, Division Director, Division of Resilience and Infrastructure Coordination, ASPR, HHS
Documentation to Use as Proof of Activity Completion: Include data or primary sources that could be used to substantiate performance of the improvement activity (e.g. medical charts, office schedules, data reports, quality improvement reports or submissions to funders/payers, meeting minutes).	Installation of the cybersecurity software and tools. Example: If a clinician did email phishing training, the clinician could prove this was completed by virtue of implementing the anti-phishing software. This could also be depicted in documentation that employees were trained. Finally, installed software could depict how alerts are treated and the number of devices that are encrypted.
Level of Effort: Include data, primary sources or personal experience to substantiate the level of effort the submitter anticipates are required to	https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5522514/ https://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf

complete the proposed improvement activity on an annual basis. (This estimate could be in hours/days, dollars, staffing needs/FTE, external resources/supports or any combination thereof).	
Contribute to Advancing Care Information Bonus: Yes or no. Yes responses require a justification/rationale—100 words or less. Improvement activities may be considered for the Advancing Care Information bonus if the improvement activity can be accomplished using Certified Electronic Health Record Technology (CEHRT).	Since many of the activities can be used to support a risk assessment this could count toward the ACI bonus.