



## TLP WHITE

In this edition of Hacking Healthcare, we tackle three significant document releases that will affect numerous aspects of the healthcare sector. First, we dive into the final report issued by the Cyberspace Solarium Commission and recap a handful of recommendations that are likely to have the biggest impact on healthcare cybersecurity and incident response. Next, we briefly break down how the finalization of two Department of Health and Human Services (HHS) rules, the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule* and the *Interoperability and Patient Access Final Rule*, are set to create wholesale changes to the way that healthcare data is accessed by patients. Welcome back to *Hacking Healthcare*.

**Cyber Solarium Releases Findings and Recommendations.** Last week the Cyberspace Solarium Commission, a bipartisan group of congressmen and private sector experts, released their long-awaited final report. The report is the culmination of a years' worth of intensive study meant to answer the questions of "What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy?"<sup>1</sup> In taking an all-encompassing approach, the commission developed a comprehensive set of recommendations that touch on nearly every aspect of cybersecurity.

Coming in at 182 pages with over 80 recommendations, the report advocates the commission's vision of 'layered cyber deterrence' as the strategic path forward for the United States. Layered cyber defense is intended to "[reduce the] probability and impact of cyberattacks of significant consequence.," and outlines three broad approaches toward achieving that aim.<sup>2</sup> The approaches include 'shaping behavior' by working internationally to promote responsible behavior in cyberspace, 'denying benefits' to malicious actors by improving public-private collaboration, and 'imposing costs' by ensuring that the United States has the capability to retaliate when necessary and credibility that it will.<sup>3</sup>

At a more granular level, the 80 recommendations are helpfully organized into 6 pillars, which all support one or more of the three approaches listed above. The pillars include 1) Reform the U.S. Government's Structure and Organization for Cyberspace 2) Strengthen Norms and Non-Military Tools 3) Promote National Resilience 4) Reshape the Cyber Ecosystem 5) Operationalize Cybersecurity Collaboration with the Private Sector and 6) Preserve and Employ the Military Instrument of National Power.

March 17th, 2020

Within these pillars are several key recommendations that have relevance to the healthcare sector:

- Recommendation 3.1.2 would “establish a national cybersecurity assistance fund to ensure consistent and timely funding for initiatives that underpin national resilience.” This fund would be available for investment into mitigations and resiliency into serious threats to public health and safety.
- Recommendation 3.3 argues for the “[codification of] a “Cyber State of Distress” tied to a “Cyber Response and Recovery Fund” to ensure sufficient resources and capacity to respond to significant cyber incidents.” Citing the lack of federal mechanisms to adequately respond to major cyber incident, a cyber state of distress would be a declaration “exclusively for responding to, or preemptively preparing for, cyber incidents whose significance is above “routine” but below what would trigger an emergency declaration.” Funding would “augment or scale up government technical assistance and incident response efforts” to critical infrastructure.
- Recommendation 4.1 outlines how Congress “should establish and fund a national cybersecurity certification and labeling authority empowered to establish and manage a program for voluntary security certifications and labeling of information and communications technology products.”
- Recommendation 4.2 may be of concern to some sectors of the healthcare sector as it pushes Congress to “pass a law establishing that final goods assemblers of software, hardware, and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities”
- Recommendation 4.4 tasks DHS with funding and directing a research and development center focused on “developing certifications for cybersecurity insurance products.” This comes as the commission acknowledges “an inability on the part of the insurance industry to comprehensively understand and price risk, due in part to a lack of talented underwriters and claims adjusters and the absence of standards and frameworks for how cyber risk should be priced.”
- Recommendation 5.1 describes how “Congress should codify the concept of “systemically important critical infrastructure,” whereby entities responsible for systems and assets that underpin national critical functions are ensured the full support of the U.S. government and shoulder additional security requirements consistent with their unique status and importance.”

The full report can be found at [solarium.gov/report](https://solarium.gov/report).

**HHS Finalizes “Historic” 21st Century Cures Act Rule and Interoperability and Patient Access Rule.** Last week, HHS finalized two “transformative rules that will give patients unprecedented safe, secure access to their health data.”<sup>4</sup> The Office of the National Coordinator for Health Information Technology (ONC) released the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule*, and the Centers for Medicare & Medicaid Services (CMS) released the *Interoperability and Patient Access Final*

March 17th, 2020

*Rule.* These long-awaited finalizations will create wholesale changes to how patient data is accessed and shared over the coming years.

ONC's final rule on the 21<sup>st</sup> Century Cures Act promotes itself as empowering patients by giving them greater access to their health data, improving patient privacy and security, and easing the ability to "shop for care and manage costs."<sup>5</sup> For clinicians and hospitals, ONC touts the benefits of a streamlined way for patients to access health data as easing the strain on staff, as well as the creation of a competitive marketplace for healthcare apps.

Other key features the rule lays out include outlining "reasonable and necessary activities that do not constitute information blocking while establishing new rules to prevent "information blocking" practices."<sup>6</sup> Furthermore, it "requires electronic health records to provide the clinical data necessary, including core data classes and elements, to promote new business models of care," and "advances a standardized set of health data classes and data elements referred to as the U.S. Core Data for Interoperability."<sup>7</sup> Finally, the rule "establishes secure, standards-based application programming interface (API) requirements to support a patient's access and control of their electronic health information."<sup>8</sup>

CMS's final rule finalizes a number of policies that provide for better interoperability across the healthcare system and facilitate patient access to healthcare information. The new policies address Patient Access APIs, Provider Directory APIs, Payer-to-Payer Data Exchanges, Public Reporting and Information Blocking, Digital Contact Information, and several others that begin to take effect in stages from 2020 through 2022. The 474-page final rule details each of the new policies including sections on technical standards, content and vocabulary standards, API standards, and background information

### ***Congress –***

Tuesday, March 17th:

- No relevant hearings

Wednesday, March 18th:

- Senate – Committee on Health, Education, Labor and Pensions - Hearings to examine an emerging disease threat, focusing on how the U.S. is responding to COVID-19, the novel coronavirus, part 2.

Thursday, March 19th:

- No relevant hearings

### ***International Hearings/Meetings –***

***EU – No relevant hearings/meetings***

### ***Conferences, Webinars, and Summits –***

--H-ISAC Monthly Member Threat Briefing – Webinar (3/31/2020)

<https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-6/>

--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (4/20/2020)

[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/426497](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497)

March 17th, 2020

- H-ISAC 2020 Spring Summit – Tampa, FL (5/11/2020 – 5/15/2020)  
<https://h-isac.org/summits/strike-back-summit/>
- H-ISAC Security Workshop - Frederick, MD (6/9/2020)  
<https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/>
- AAMI Exchange – New Orleans, LA (6/12/2020-6/15/2020)  
<https://h-isac.org/hisacevents/aami-exchange/>
- H-ISAC Security Workshop - Lisbon, Portugal (6/17/2020)  
<https://h-isac.org/hisacevents/h-isac-security-workshop-lisbon-portugal/>
- H-ISAC Security Workshop - Buffalo, NY (6/23/2020)  
<https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny-2/>
- H-ISAC 2020 Inaugural APAC Summit – Singapore (6/23/2020-6/25/2020)  
<https://h-isac.org/summits/apac-summit-2020/>
- Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)  
[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/426499](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499)
- Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)  
[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/426517](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517)
- H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020)  
<https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-village-co/>
- Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)  
[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/427126](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126)
- Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)  
<https://h-isac.org/hisacevents/summit-on-security-third-party-risk/>
- Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)  
[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/428840](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840)
- H-ISAC Security Workshop - Mounds View, MN (10/27/2020)  
<https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/>
- Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)  
[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/428886](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886)
- Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)  
<https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/>

### ***Sundries –***

**--Coronavirus: 3D printers save hospital with valves**

<https://www.bbc.com/news/technology-51911070>

**--Microsoft delivers emergency patch to fix wormable Windows 10 flaw**

<https://arstechnica.com/information-technology/2020/03/microsoft-delivers-emergency-patch-to-fix-wormable-windows-10-flaw/>

**--A coronavirus-tracking app locked users' phones and demanded \$100**

<https://www.cyberscoop.com/coronavirus-app-locked-phones/>

**--Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak**

<https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response?sref=P635h0rP>

Contact us: follow @HealthISAC, and email at [contact@h-isac.org](mailto:contact@h-isac.org)

March 17th, 2020

---

<sup>1</sup> <https://www.solarium.gov/report>

<sup>2</sup> <https://www.solarium.gov/report>

<sup>3</sup> <https://www.solarium.gov/report>

<sup>4</sup> <https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html>

<sup>5</sup> <https://www.healthit.gov/curesrule/what-it-means-for-me/patients>

<sup>6</sup> <https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html>

<sup>7</sup> <https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html>

<sup>8</sup> <https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html>