June 6, 2022

Honorable. Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

RE: Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended
RIN 0945-AA04

Comments Submitted Electronically via Regulations.gov

Dear Secretary Becerra:

The Healthcare and Public Health Sector Coordinating Council (HSCC) welcomes the opportunity to submit comments in response to the Office for Civil Rights (OCR) at the Department of Health and Human Services' Request for Information (RFI) on the *Considerations for Implementing the Health Information Technology for Economic and Clinical (HITECH) Act.*

The HSCC is a private sector-led critical infrastructure advisory council of large, medium and small health industry stakeholders working with government partners to identify and mitigate threats and vulnerabilities affecting the ability of the sector to deliver healthcare services to our nation's citizens. A major component of the HSCC is its Cybersecurity Working Group, which represents 300 healthcare organizations in the subsectors of direct patient care, medical materials, health information technology, health plans and payers, laboratories, biologics and pharmaceuticals, and public health. Our members collaborate toward improving the cyber security and resiliency of the healthcare industry and patient safety.

Applicability of the New Law

The private-sector members of the HSCC support the department's efforts to implement Public Law 116-321 which directs the U.S. Department of Health & Human Services (HHS) to consider evidence of Recognized Security Practices as a mitigating factor when resolving an investigation of a complaint or compliance review for suspected violations of the Health Insurance Portability & Accountability Act (HIPAA) Administrative Simplification provisions.

As a broad policy approach we recommend that OCR produce guidance that defines what are considered 'recognized cybersecurity practices', that are practical, implementable, and set in partnership with the healthcare industry. Specifically, we recommend further definition of 405(d) practices in collaboration with OCR so that 'recognized cybersecurity practices' can be tailored to the various sizes, structures and security functions of the multifaceted healthcare industry.

The HSCC recognizes that PL 116-321 could be viewed to apply to enforcement actions taken by the Secretary that are outside the authority delegated to OCR.[1] For example, section 1176 of the Social Security Act empowers the Secretary to issue fines for a covered entity's violation of the Administrative Simplification standards for the use of unique health identifiers and the standardization of code sets in

[1] Under the authority of Sections 1171 through 1180 the Secretary promulgated standards for unique health identifiers and transactions and code sets at 45 CFR Parts 160 and 162. The Secretary delegated the administration and enforcement of these standards to the Administrator for CMS.

certain electronic transactions.[2] We point out that the RFI does not address the application of PL 116-321 to actions taken by the attorney general of a state to enforce the HIPAA standards.[3] It is our understanding that it was the intent of the congressional sponsors of PL 116-321 to apply the provisions to enforcement actions and audits for compliance with the HIPAA privacy and security standards.[4]

45 CFR Part 160, Subpart D establishes the Secretary authority for the imposition of a civil money penalty and the procedures to be followed in taking action.[5] The Enforcement Rule requires the Secretary to consider a number of mitigating factors[6] and affirmative defenses[7] in determining the amount of a civil monetary penalty. The intent behind the requirements of PL 116-321 could be read as direction from Congress on factors to be considered and affirmative defenses when applying the Enforcement Rule specifically to alleged violations of the HIPAA Privacy and Security standards.

We note that there have been no regulations adopted to implement Section 13411 of the HITECH Act which mandated the Secretary to establish a program to audit covered entities and business associates compliance with the HIPAA privacy, security and breach notification standards. Through sub-regulatory guidance OCR developed a limited audit program to assess the controls and processes covered entities have implemented to comply with them.[8] To date, OCR has not disclosed if an enforcement action has been taken against a covered entity or business associate as a direct result of a HIPAA compliance audit.

We recommend OCR implement the provisions of PL 116-321 through issuance of regulatory guidance and adopt internal policies for case management to afford enforcement discretion regarding use of security best practices as it applies to safeguarding protected health information (PHI). This approach will provide the most benefit to the healthcare industry, incentivizing the adoption of recognized security practices, and other frameworks recognized by NIST captured in their National Online Informative References Program, while avoiding interference with the other areas of the HIPAA Administrative Simplification provisions.

Responses to Select RFI Questions

Question 1: ***What recognized security practices have regulated entities implemented? If not currently implemented, what recognized security practices do regulated entities plan to implement?***

Response: There are numerous recognized security practices that our sector employs to manage risk and which they use to comply with HIPAA. In a survey of our sector's membership that are HIPAA covered entities or business associates, the breakdown was the following:

While not necessarily a representative sample of the segment of the healthcare sector that are covered entities or business associates, it does offer a general idea of the frameworks in use and suggests that HIPAA itself – while not technically a framework – is still the path many entities, especially small and

[2] 45 CFR Part 160 Subparts C & D (collectively known as the Enforcement Rule) addresses Secretarial action regarding complaints and compliance reviews, and the imposition of civil money penalties for failure to comply with parts 160, 162 and 164.
[3] See SSA Section 1176(d)
[4] 45 CFR Parts 160 and 164, Subparts C & E.
[5] For purposes of this discussion, we assume subpart D permits the Secretary to enter into voluntary settlement agreements with covered entities and business associates to resolve violations of the HIPAA standards.
[6] See 45 CFR 160.408 Factors considered in determining the amount of civil money penalty.
[7] See 45 CFR 160.410 Affirmative defenses.
[8] See the HIPAA Privacy, Security, and Breach Notification Audit Program | HHS.gov Last viewed May 26, 2022.

medium sized ones – take in attempting to manage their risk. The responses also reflect strong adoption of the NIST Cybersecurity Framework (CSF) and 800-53 which we know from previous polling of the entire sector is widely used. Finally, we are pleased to see what we know to be a growing use of the Health Industry Cybersecurity Practices (HICP), a NIST CSF-aligned resource published January 2, 2019 by the Health Sector Coordinating Council's "405(d)" Task Group following more than one year of pre-testing. The 405(d) Task Group is a joint effort by HHS and the HSCC, and is one of currently 15 task groups of the HSCC Cybersecurity Working Group.. Hundreds of HSCC members have contributed to developing the HICP and it enjoys widespread support among the HSCC members.

- HIPAA - 77.7%
- NIST CSF - 72.2%
- HICP/405(d) - 61.1%
- NIST 800-53 - 50%
- ATT&CK (MITRE) - 13.8%
- CIS 18/20 - 13.8%
- ISO 2000/1 - 8.3%
- ISO 14971 - 8.3%
- CMMS (Microsoft) - 5.5%
- FIPS 200 - 5.5%
- Other -22.2%

Question 5: ***What steps do covered entities take to ensure that recognized security practices are "in place"?***

Our member survey found that 83 percent are implementing a risk assessment, 27.8 percent are mapping to the 405(d) best practices, 25 percent are conducting continuous assessment platform implementation, and 16.7 percent are employing something other than these methods.

It is important to keep in mind the resource constraints of our sector which has received a devastating blow as a result of the COVID-19 pandemic. In addition to fighting what were already growing cybersecurity threats prior to 2020 at the start of the pandemic, many providers are facing crippling workforce shortages. Furthermore, cyber criminals have opportunistically used the pandemic to their advantage, levying an unprecedented number of ransomware attacks. According to the U.S. Department of Health & Human Services' (HHS) own Ransomware Trends Report, less than halfway through 2021 our sector saw 48 ransomware incidents targeting our sector.[9] Consider also these statistics:[10]

- The HIPAA breach website shows 713 breaches reported in 2021, affecting PHI from more than 45.7 million patient records.
- At least 526 of the 713 breaches reported in 2021 were categorized as Hacking/IT Incidents which affected 43.1 million records, or 94 percent of the total records breached in 2021.

Question 6: ***What steps do covered entities take to ensure that recognized security practices are actively and consistently in use continuously over a 12-month period?***

Sixty-six point seven (66.7%) percent who responded to our survey are implementing a risk assessment, 63.9% percent are conducting routine external audits and testing, 30.6% are engaging in a continuous assessment platform implementation, and 19.4% are using something other than these

[9] https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf
[10] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

methods.

Conclusion

The issuance of regulatory guidance and the adoption of internal policies to afford case management enforcement discretion regarding the use of security best practices will benefit the healthcare industry by further incentivizing the adoption of recognized security practices while avoiding interference with the other areas of the HIPAA Administrative Simplification provisions as it applies to safeguarding protected health information (PHI).

If you have any questions related to our letter or would like to discuss our letter further, please contact Greg Garcia, Executive Director, Healthcare and Public Health Sector Coordinating Council at greg.garcia@healthsectorconcil.org.

Sincerely,

Greg Garcia
Executive Director
Health Sector Coordinating Council Cybersecurity Working Group