June 6, 2022

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

Comments Submitted Electronically via Regulations.gov

Dear Secretary Becerra:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) welcome the opportunity to submit comments in response to the Office for Civil Rights at the Department of Health and Human Services' Request for Information on the *Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act.*

CHIME is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders. Consisting of more than 2,900 members in 60 countries, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. Launched by CHIME in 2014, AEHIS represents more than 950 healthcare security leaders and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members are among the nation's foremost health IT experts, including on the topics of cybersecurity, privacy and the security of patient and provider data and devices connecting to their networks.

OCR is issuing this RFI to improve its understanding of how covered entities and business associates (regulated entities) are voluntarily implementing recognized security practices as defined in Public Law 116-321. CHIME and AEHIS are strong supporters of the new statute which gives the Secretary of the U.S. Department of Health & Human Services (HHS) the authority to take into account providers and other HIPAA covered entities who use recognized security practices, including those under 405(d), when levying fines, audits and other remedies in response to a possible HIPAA security rule violation.

We appreciate OCR seeking stakeholder feedback to help inform how this new law can be leveraged in practice including understanding how covered entities and business associates are voluntarily implementing recognized security practices. Below are our responses to OCR's questions.

RFI Responses

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:

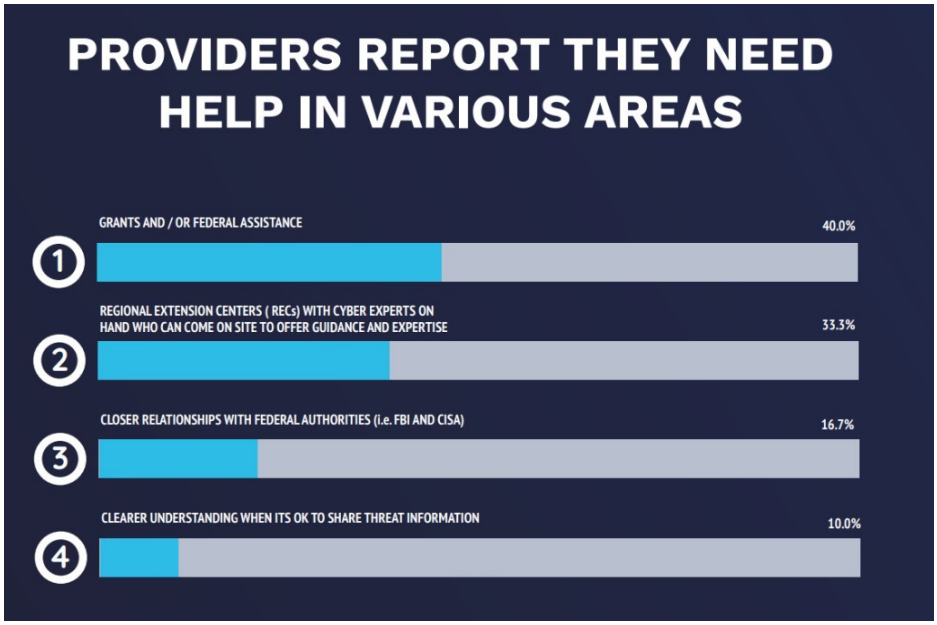
The statute defines "recognized security practices" to mean:

> *the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the covered entity or business associate, consistent with* the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title).

As identified in the statute's definition, there are indeed several standards, best practices and procedures in place and healthcare providers rely on these today to implement enterprise risk management best practices. As avid champions and active members of the community that has helped develop the cybersecurity best practices developed under 405(d) cybersecurity fostered through a public-private partnership, we believe there is a very strong role this set of best practices can play in strengthening the cybersecurity resiliency of our sector. However, we also recognize that there are other practices that providers, other covered entities, and business associates may be already using to best manage their risk. We believe that it is important for providers to have the latitude to apply the standards and procedures they believe best meet their organization's needs. We even have some members who have adopted practices that exceed those recommended under 405(d).

We understand that levying enforcement discretion should ideally be accompanied by both policy incentives and penalties so as to further encourage and support providers in making these critical investments. That said, the nation continues to navigate a pandemic that has lasted far longer than anyone would have imagined, and it is important to balance the requirements on providers with their operational needs to provide lifesaving care. COVID-19 continues to claim lives as criminals and hostile nation states leverage the pandemic to their advantage exacting a serious, additional toll on an already stressed system. The pandemic has opened the door to new threatscapes as these bad actors relentlessly attack our critical infrastructure as the beleaguered healthcare workforce continues to navigate the evolving nature of this virus. We believe it is thus important to be practical as the sector tries to recover from the seemingly unending strain of COVID19.

The other pressing matter that is facing our sector are limited resources. We cannot state this point enough. Healthcare providers were already strained prior to the pandemic with limited resources - and for the smallest often none - creating ongoing opportunities for the aforementioned criminals. Ransomware has become a household name among hospitals and other providers as they are "target rich and cyber poor." In a recent survey[1] of our members last year we found that among respondents, 67% had suffered a cyber incident in the past twelve months. Our survey further highlighted the desperate need for assistance for our sector. Forty percent of respondents said they could use support in the form of grants or federal assistance.



Recommendations: OCR should:

1. Allow healthcare providers to adopt NIST-based framework / standards consistent with the language in the statute so long as they demonstrate adherence to that framework through an annual assessment and attestation that they are working to address identified material deficiencies;
2. Require an independent review / third-party assessment to verify the framework / standards the option for a waiver for organizations who attest they are under-resourced and unable to afford this. Take into account the financial ability of a healthcare provider to manage risk and to adopt strategies to address deficiencies;
3. In the case of small and / or under-resourced providers, exercise flexibility when determining enforcement action and offering credit for the use of standards and best practices; and
4. Appropriate credit should be given to those forward leaving providers who have adopted practices that exceed those recommended under 405(d).

Question 2: ***What standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the NIST Act do regulated entities rely on when establishing and implementing recognized security practices?***

Response:

Among our members, the NIST CSF continues to be strongly supported and widely used. Some of our members utilize the NIST Risk Management Framework and associated Special Publications (e.g. 800-53, 800-37, etc.). Others also report that HIPAA is being used which we understand is not technically a cybersecurity framework, however, especially for small and medium providers this is what they use to manage their risk.

The 405(d) best practices, tied to the NIST CSF, are also beginning to get traction among our members. While this is a newer set of tools, awareness and use are growing among providers and it is beginning to permeate the healthcare landscape as more providers adopt them or prepare to adopt them. Our recent survey data also found 55% percent of survey respondents are aware of the new best practices.

While use of the best practices developed under 405(d) is growing, more work is needed to increase awareness of these tools. Our survey also found low awareness of PL 116-321 with only 37% of respondents indicating familiarity. CHIME and AEHIS continue to educate members about this important new legislation. More education efforts by HHS are needed to help educate providers about the 405(d) best practices. And, more awareness is needed by small and lesser-resourced providers of tools that are free from the federal government like those available from CISA on risk assessment and their cybersecurity hub.

Question 3: ***What approaches promulgated under section 405(d) of the Cybersecurity Act of 2015 do regulated entities rely on when establishing and implementing recognized security practices?***

Response: The answer to this varies depending on the provider. There are ten cybersecurity best practices contained in 405(d)'s Health Industry Cybersecurity Practices broken down into further sub-practices. Providers select the measures that most meet their needs. If there was one area of focus that we believe small providers should begin by adopting, it would be around access management. Just beginning to stop sharing passwords, institute strong passwords and putting in place access management would be a big step in the right direction.

It's important to keep in mind that most providers who have started to adopt cybersecurity best practices or follow a framework are on a journey and that cyber hygiene is a journey, not a destination. You are unlikely to find most healthcare providers have adopted all the best practices and no provider can ever safely conclude that they are at the end of their cybersecurity journey. Even for better resourced providers, cybersecurity is an ongoing and expensive effort, and many are just beginning to scratch the surface when it comes to measuring their progress.

Question 4: ***What other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities do regulated entities rely on when establishing and implementing recognized security practices?***

Response:
The NIST CSF continues to be the most widely adopted framework across critical infrastructures and internationally.

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

Response: Depending on size, the nature of risk (depending on a covered entity's / business associate's size, revenue, and number of patient records) there should be a cycle during which a risk assessment should have been performed.

Recommendation: We recommend this be between one to three years, or in the event of a significant change to the environment or threat landscape (i.e., attack, merger, pandemic, work from home).

Response:

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?***

Response:

Providers often conduct third party risk assessments tied to a specific framework such as the NIST CSF. They also set organizational policy related to information security and the use of security controls that flow from one of the recognized frameworks.

More sophisticated organizations also measure not only the existence and efficacy of a security control, but also the completeness of the control's implementation. Most healthcare delivery organizations have equipment that is outside of the span of control of the IT organization (e.g., vendor owned/managed). In these cases, there is a need for expanded coordination and often compensating controls to ensure the organization understands and appropriately manages the risk to their information.

Question 7: ***The Department requests comment on any additional issues or information on the Department should consider in developing guidance or a proposed regulation regarding the consideration of recognized security practices.***

Response: In considering how to enforce breaches, we believe it is imperative that OCR consider the implications of cyber weaknesses of medical devices and the ongoing challenges that these present not only to patient privacy and security but also to patient safety. We are strong supporters of the PATCH Act (H.R. 7084 and S. 3983) which would grant the Food and Drug Administration (FDA) explicit authority to require manufacturers who submit for a premarket approval for a cyber device to meet cyber requirements. Equally important is the FDA has requested this authority from Congress in their FY23 budget submission. In their Executive Summary of FY 2023 Legislative Proposals budget document, the agency requests:

> *Currently there is no statutory requirement (pre- or post-market) that expressly requires medical device manufacturers to address cybersecurity, yet cybersecurity incidents put patients at great risk, and also have the potential to cause supply chain disruptions that can cripple our health care system. This proposal would advance medical device safety by explicitly requiring that medical device manufacturers design cybersecurity into their devices and by ensuring that FDA and the public have certain information about device cybersecurity. Specifically, FDA seeks to have express authority to require: that premarket submissions to FDA include evidence demonstrating reasonable assurance of the device's safety and effectiveness for purposes of cybersecurity; that marketed devices demonstrate a reasonable assurance of the device's safety and effectiveness for purposes of cybersecurity; that devices have the capability to be updated and patched in a timely manner; that manufacturers provide a device Software Bill of Materials (SBOM) with their devices so users know which components of their devices are or may be subject to cyber threats; and that device manufacturers publicly disclose when they learn of a cybersecurity vulnerability so users know when a device may be vulnerable, and to provide direction to users to reduce their risk. These authorities are critical, as FDA has already seen and responded to several ransomware and other malware incidents within the health care*

sector. Stronger cybersecurity protections are necessary to ensure we remain prepared to protect patients and our health care workers on the front lines. Enacting FDA's proposal would reduce the likelihood of harm to patients, interrupted access to devices, and loss of market share or market withdrawal for devices for which a vulnerability is identified as a result of cybersecurity incidents.

The FDA has also recently released a new Premarket Draft Guidance on Cybersecurity of Medical Devices which has an increased focus on ensuring devices are adequately secure. CHIME & AEHIS applaud these efforts by the Administration and Congress and urge OCR to take into consideration the impact breaches stemming from medical devices have and the limited ability providers have in safeguarding patient privacy when they are forced to purchase devices off the shelf that arrive with known vulnerabilities.

Conclusion

CHIME & AEHIS appreciate the opportunity to lend our voice to the policymaking process and if you have any questions related to our letter or would like to discuss further, please contact Mari Savickis, Vice President of Public Policy, at mari.savickis@chimecentral.org.

Sincerely,

Tanya Townsend, CHCIO
CHIME Board Chair, SVP & CIO
Louisiana Children's Medical Center

Sri Bharadwaj, MS, FCGMA, FHIMSS, CPHIMS, CISSP, CLSSBB, PMP, CHCIO
Chief Operations and Information Officer
Longevity Health