June 6, 2022

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

The Honorable Lisa J. Pino  
Director  
Office of Civil Rights  
U.S. Department of Health & Human Services,  
200 Independence Avenue, S.W.  
Washington, D.C. 20201

RE: Request for information certain provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act and Impact and Need of Providers in Underserved Communities

Dear Secretary Becerra and Director Pino,

On behalf of OCHIN, I appreciate the opportunity to comment on the U.S. Department of Health and Human Services Office of Civil Rights’ (OCR) Request for information on recognized security practices of covered entities and business associates that should be considered as part of rulemaking as part of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. OCHIN is a national health information technology innovation and research network that that serves nearly 1,000 community health care sites with 21,000 providers in 47 states, serving more than 6 million patients including federally qualified health centers (over 100), community health clinics, Ryan White HIV/AIDS Program Health Centers, school-based health clinics, Tribal health clinics, local public health agencies, and critical access hospitals.

Driving Equitable Access

For over two decades, OCHIN has advanced equitable health care solutions by leveraging the strength of our network’s unique data set and the practical experience of our members to drive knowledge solutions for patients and providers in underserved communities. OCHIN members serve on average over 130,000 patients each month. Fifty percent of our members’ patients are covered by Medicaid, one out of three prefer care in language other than English, and three out of five network patients have chronic conditions.1 Annually, OCHIN members digitally exchange over 200 million clinical summaries securely across all 50 state and the District of Columbia.

---

1 OCHIN Epic patients only.
Prioritizing Cybersecurity for Providers in Underserved Communities

OCHIN network members have the option to seek OCHIN cybersecurity assessment services which include targeted penetration testing and vulnerability assessments. OCHIN works with members to develop a focused action plan that identifies risks and provides members with tools, so they are able to comply with privacy and security regulations. These services reflect decades of expertise OCHIN has developed serving health IT needs of providers in underserved communities that face under-investment and serve patients with the highest social risks (structural inequality) and are medically complex (multiple co-morbidities). Further, our members serve patients who are at heightened risk of harm when a breach occurs. For example, when a patient’s identity is compromised due to a breach, the patient may have few resources to address the harmful consequences. Such breaches can exacerbate structural inequality for patients in underserved communities. In addition, such breaches can worsen the financial challenges faced by safety-net providers that have relatively fewer resources and funding as compared to providers serving commercially insured patients or large health systems. The latter receive funding for serving under insured or uninsured patients through several mechanisms (such as, for example, federal health care program disproportionate share hospital payment adjustments, loss on sale adjustments, bad debt adjustments, research funding, and relatively higher mix of Medicare and commercially insured patients).

Key Recommendations:

1. In light of the rapidly escalating incidence and severity of cybersecurity threats to community health clinics and other safety net providers, the U.S. Department of Health & Human Services (HHS) must swiftly move forward to provide ongoing sustained funding for providers in underserved communities, so the latter are able to immediately strengthen their cybersecurity measures as well as to support their adherence to any future changes to the HIPAA Security Rule.

Because of the persistent underfunding faced by providers in underserved communities, resources are not available to upgrade their IT systems and associated cybersecurity practices and programs. Passage of Section 405 of the Cybersecurity Act of 2015 demonstrated the expectation of Congress that HHS reorient its approach to working with health care providers to actively provide cybersecurity tools and resources through collaborative stakeholder engagement. As the threat landscape evolves the type of support provided by HHS should evolve as well. We urge HHS to undertake a comprehensive evaluation of existing programs and funding mechanisms and the discretion HHS has to authorize and allow for providers in underserved communities to access current program funding to cover costs for needed cybersecurity upgrades and improvements on an ongoing basis.

Federally Qualified Health Centers (FQHCs), community health clinics, critical access hospitals, rural health clinics, and other providers in underserved communities face urgent demands with insufficient payment and resources to meet the convergence of public health emergencies (COVID-19, mental health, substance abuse disorder) and structural inequality in health care and their communities. Even if clinics are able to conduct more comprehensive and rigorous assessments of their cybersecurity controls, far too many do not have the resources to undertake the needed upgrades to their systems. Furthermore, many providers in underserved communities do not have health IT trained staffing and the funding needed to convert from manual to automated security tools. We cannot wait a year to implement essential recognized security practices that are needed immediately and providers in underserved communities need ongoing financial support now.
2. **Immediate funding is needed to increase the number of cybersecurity staff among underserved providers and rebuild the community health clinic operational and support staff with health IT training that includes cybersecurity.**

Essential and basic security measures require operational and support staff with health IT training who are responsible for such systems as well as training for those who regularly use such systems in community health clinics. In California, OCHIN network members have lost 1/3 of their operational and support staff who are responsible for health IT systems or who regularly use such systems which has strained their capacity to continue to deliver health care services, build toward new payment models, and has left them with heightened cybersecurity risk. This is an urgent priority that can be addressed right now with targeted funding for health IT training for operational and support staff for community health centers and local public health agencies.

3. **Accelerate COVID-19 rescue funding to support local community health clinic, rural critical access hospital and local public health agency IT modernization.**

Too many providers remain on antiquated and legacy IT systems (including health IT systems) that leave them vulnerable and at heightened cybersecurity risk. Federal funds for infrastructure should be deployed to immediately focus on rapid replacement of legacy systems with modernized IT systems including certified health IT systems that have essential cybersecurity components.

4. **Fund state-based/regional cybersecurity extension centers to provide technical assistance, risk assessments, breach mitigation support services, and staff augmentation services for providers in underserved communities.**

Currently, the limited number of professionals with cybersecurity training and experience creates significant challenges for providers in underserved communities that seek to establish and maintain optimized cybersecurity programs. Simply stated, they are not able to compete with larger health care organizations and commercial entities across industries for trained cybersecurity staff. Furthermore, most providers lack ready access to resources to implement mitigation plans when breaches or attacks occur. HHS should take steps as part of national defense and protecting the U.S. health infrastructure to establish state-based/regional cybersecurity extension centers for providers in underserved communities so they are able to leverage economies of scale, work with centers that are able to recruit and retain cybersecurity experts, and benefit for the experience of regional centers to remain up-to-date and mitigate.

5. **Transparency is key in adopting strong cybersecurity standards. OCHIN urges OCR to establish a regulatory roadmap that ensures all stakeholders can be aware of and involved in the development of these rules.**

Putting in place strong cybersecurity regulations necessitates the involvement of stakeholders who are able to plan, prepare, and provide feedback on this complex topic. Implementing cybersecurity rules for health care providers will impact their workforce, budgets, and ability to operate. Allowing these providers, particularly those in underserved rural areas with limited technical resources and funding, to closely follow and interact with the regulatory process is an absolute necessity to ensure compliance and equitable application of any forthcoming rules. In short, providers need a specific security framework that all regulated entities must adhere to which will facilitate widespread adoption, lower costs, and improved overall system security.
6. **OCHIN strongly urges OCR to initiate rulemaking in order to establish clear guardrails that covered entities and business associates should adhere to in order to comply with HIPAA Security Rule obligations.**

   The lack of specificity of controls invites the use of standards, protocols and practices that do not provide patients and providers with essential protection needed. In short: we do not rise to the level of our goals; we fall to the level of our systems.\(^2\) This lack of regulatory clarity is placing patients who face the most significant health inequities at the greatest risk of harm and providers in underserved communities to the highest relative magnitude of costs and liability exposure.

7. **We offer several recommendations in the Appendix related to recognized industry practice, but we strongly urge OCR to require leveling up to recognized industry practice by, at a minimum, establishing vulnerability and penetration testing of security protocols and measures at least one time per year.**

   Currently, many providers have policies and stated procedures that comply with the HIPAA Security Rule but have not been tested or even regularly updated within a reasonable period of time. Regularly required vulnerability and penetration testing are necessary to avoid what can be catastrophic consequences for a community health clinic, their patients, their families, and their communities.

Please contact me at stollj@ochin.org to discuss how we can offer our expertise on this complex topic.

Sincerely,

Jennifer Stoll  
Executive Vice President  
External Affairs

---

\(^2\) Atomic Habits: An Easy and Proven Way to Build Good Habits and Break Bad Ones, James Clear
APPENDIX
Detailed Response to Questions

What recognized security practices have regulated entities implemented?

As a threshold matter, we urge OCR to consider the limited resources among small practices and providers in underserved communities. In light of the foregoing, OCHIN urges OCR to utilize commonly available and non-proprietary frameworks that allow the most resource-limited clinics and providers to adopt crucial cybersecurity measures. The cost of recovery from a cyber incident is almost always greater than the cost of preventing one, however, even this substantially lower cost is too great for many providers and clinics.

There are a range of recognized cybersecurity practices due to a number of factors ranging from targeted sector to drafting bodies that hold differing priorities. Many providers adhere to the Payment Card Industry Compliance Data Security Standards (PCI DSS) or PCI for short, due to the fact that they accept credit cards as a form of payment from patients.3 PCI is not a health care focused standard, rather it revolves around finance and, as the name suggests, payment cards. However, the standard overlaps with and exceeds many HIPAA cybersecurity requirements. PCI standards include the following 12 core guidelines:

- Implement firewalls to protect data
- Appropriate password protection
- Protect cardholder data
- Encryption of transmitted cardholder data
- Utilize antivirus software
- Update software and maintain security systems
- Restrict access to cardholder data
- Unique IDs assigned to those with access to data
- Restrict physical access to data
- Create and monitor access logs
- Test security systems on a regular basis
- Create a policy that is documented and that can be followed4

While PCI is not intrinsically linked to health care, the requirements for PCI provide some of the same protections required under HIPAA, such as requiring risk assessments, entry and exit processes, awareness and training programs, and physical and device security, for example. HIPAA has a more broad and loose structure than PCI, meaning PCI offers clear and specific security standards in contrast to the HIPAA standards. The latest version of PCI5 has 292 requirements and 1,030 validation points while HIPAA has 157 requirements and 535 validation points spread across the Security, Breach, and Privacy rules. Every requirement contains several validation points. For example, utilizing antivirus software is a requirement, teaching management how to use it, regularly checking for patches, and reviewing policy documentation would all be validation points. This stark difference in the quantity of requirements and

---

3 OCHIN utilizes the NIST Security and Privacy Controls for Information Systems and Organization Special Publication 800-53, known as 800-53 Moderate for a host of organizational reasons.
4 https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1652383287170
5 https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1652383287170
validations demonstrates just how loose a framework HIPAA is; it does not clearly delineate how exactly a covered entity is supposed to implement a cybersecurity policy.

While PCI DSS is certainly a good standard, it does not contain all of the same requirements that HIPAA does, meaning providers can still acknowledge certain security features even after a thorough implementation of PCI, such as patient rights and confidentiality among authorized users of a patient’s file. This gap of coverage is why a stricter standard is required for covered entities and business associates, as HIPAA can be too nebulous and PCI, while suitable for many applications, falls short when dealing with protected health information (PHI).

In addition to the various frameworks, industry practice includes mandatory and forced patching on a regular basis. By being specific on a control, for example, requiring that critical patches must be applied within a specified number of business days, organizations are able to ensure all practices implement a measurable goal that can be continually tested and reported. OCR guidance does not set this specific period for this control. Returning to the PCI comparison, PCI Requirement 6.2 specifies “prioritizes critical infrastructure fixes, ensuring that as soon as a patch is issued, high-priority networks and devices are protected from vulnerabilities.” Following this example, OCHIN recommends prioritizing patch installs so that security updates are deployed within 30 days and other low-risk patches within 2-3 months for sensitive or at-risk systems. HIPAA requires patching, but it makes no mention of timelines or maximum allowable duration prior to installing a patch following its release. This broad standard results in security flaws going unpatched for years in certain circumstances. Having a rigorous and clearly defined maximum allowable time between when a patch is released and when it must be applied by the end user is critical for ensuring simple flaws like zero-day exploits are not still available to bad actors two years after they have been discovered and fixed by the software developers. PCI DSS once again beats HIPAA by requiring patches be installed within 30 days of their release, setting a good precedent to follow for the development of widespread standards.

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?

The National institute of Standards and Technology (NIST) cybersecurity framework is largely considered the best practice when it comes to establishing and implementing cybersecurity. The framework provides an excellent starting point for covered entities and others to establish their cybersecurity infrastructure while adhering to industry standards that have been vetted by a trusted source. The NIST frameworks offer a step-by-step guide for implementing a robust and effective cybersecurity infrastructure. Of the various frameworks some provide more detail or strenuous requirements than others. This creates an imbalance in cybersecurity preparedness when neighboring clinics operate on two different levels of protection. Having a lower standard reduces security for all parties involved, as providers and clinics regularly share data between themselves and with other practices that may not adhere to the same NIST standard.

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?

As previously discussed, PCI DSS is a trusted and vetted cybersecurity framework that many covered entities utilize to partially comply with HIPAA. While this framework is not regulatory or legal, and is in-
fact, proprietary, it is nonetheless an effective and widely used method of ensuring financial transactions are protected, thus also covering HIPAA related security requirements. PCI DSS is not the only framework that fits that description, however. Another useful framework that is seeing growing adoption outside of its principal users is System and Organization Controls (SOC 2)6.

SOC 2 is a security framework developed by the American Academy of Certified Public Accountants. Similar to PCI DSS, SOC 2 is a finance-driven cybersecurity framework rather than a health-focused one. In this sense, SOC 2 does not fully encompass what HIPAA requires of covered entities, but it does require a robust and individualized framework. Additionally, SOC 2 is designed for cloud-based security. This is particularly relevant as electronic health records have become the standard for health data sharing and transfer, and many EHRs are cloud-based to allow for various points of access. SOC 2 is a framework which defines criteria for protection and managing consumer data based on several principles7 and their (non-exhaustive and sometimes duplicative) sub-requirements:

- **Security**
  - Network/Application Firewalls
  - 2FA
  - Intrusion Detection
- **Availability**
  - Performance Monitoring
  - Disaster Recovery
  - Security Incident Handling
- **Processing integrity**
  - Quality Assurance
  - Processing Monitoring
- **Confidentiality**
  - Encryption
  - Access Controls
  - Network/Application Firewalls
- **Privacy**
  - Access Controls
  - 2FA
  - Encryption

Organizations using SOC 2 are required to implement a unique and individualized instance of the framework that best controls for and protects the aspects of their business. This customizability makes SOC 2 extremely useful for covered entities that need to blend both HIPAA requirements and other cybersecurity needs, such as protecting financial transactions. SOC 2 is particularly important for covered entities because of the rigorous auditing and reporting requirements in the framework.

**What steps do covered entities take to ensure that recognized security practices are “in place”**?

The ability to ensure cybersecurity measure are “in place” varies from organization to organization. And depends heavily on their systems integration and controls. Industry practices are varied, but the following

6 [https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html](https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html)
are examples of broad policies that work to enhance cybersecurity and that can apply to almost any organizational IT infrastructure:

• Centralized provisioning and management of computers being added to the corporate network. The automation of provisioning enforces the application of computer policies such as enabling of firewalls, rotating of local administrative accounts, management of security settings and the limiting or authorizing of which applications can run on a corporate computer.

• Centralized inventory of computers, servers and applications installed within the corporate environment to help staff manage the updating of known security patches for applications, operating systems, drivers, and firmware. Central management allows risk to be monitored and critical vulnerabilities to be mitigated rapidly, as knowing that a specific application is installed on two or five hundred machines allows patching and management of the application in a controlled pattern. Many security vulnerabilities are not identified because companies do not understand their application or firmware inventory.

• Vulnerability scanning and penetration testing is implemented to identify known security flaws in systems and additionally identify vulnerable configurations of systems that have been correctly patched. For example, an operating system has been patched with the latest security patches from the vendor, but a service is enabled that grants access to the files on the computer without a need to authenticate. Additionally, a new device is installed on a network but the default passwords have not been changed. By conducting these tests regularly providers are demonstrating that they have implemented part of the Risk Analysis duties required by HIPAA. In addition to the foregoing, organization vulnerability scanning is conducted against the network every 72 hours and penetration testing is conducted both externally and internally annually at a minimum.

• Requiring regular password changes (every 90 days) across all systems. While this has been considered best practice in the industry for many years, studies have shown that frequently changing strong passwords that a user must remember leads to poor password hygiene. OCHIN recommends that any universal framework address frequent password changes, which can increase the vulnerability of passwords. Any forthcoming framework should be aligned to modern standards on the frequency of rotation of passwords as outlined in NIST Special Publication 800-63B.

• Accepted best practice requires multi-factor authentication in combination with username and password to increase security. Microsoft reported that MFA, which requires that users authenticate with at least two factors, can reduce the risk of identity compromise by as much as 99.9 percent over passwords alone.

• Password lengths for administrative accounts should be longer than normal user accounts. Administrative accounts should be at minimum 15 characters long and utilize multi-factor authentication tokens.

• Implement the principle of least privilege ensuring that only those who are authorized to access or modify a system are able to so. Best practices involve not giving users local administrative control of their computer, limiting the ability to install unauthorized software, limiting access to sensitive data and files, and reducing exposure to malware.

• Implementation of File Integrity Monitoring (FIM) solutions allow the detection of modification or deletion of critical configuration files, operating system files or files containing sensitive data.

• Installation of protections that scan every URL and attachment shared through corporate email or shared services should be implemented to both open attachments and URL (links) in a sandbox.
separate from the corporate network to determine if a malicious payload is attached. If the payload is malicious the email or shared file is removed before delivery.

- Backups are implemented using the standard 3-2-1 process. (Create one primary backup and two copies of your data. Save your backups to two different types of media. Keep at least one backup file offsite.) And, test restorations should be conducted on all critical systems every 6 months to make sure you can restore from every source in an event.
- Budget and Replace end-of-life or end-of-support hardware and software before it is no longer supported by vendors. For example, if you are still running Windows XP on your desktop in a corporation it’s too late and an update is necessary to ensure security due to the fact that Microsoft no longer offers security updates for Windows XP.

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

Over time, there can be a significant change in workforce, trainings fade, and software changes. All of these factors necessitate the regular and required training of employees in best practices. Regular, (on hiring, annually or more frequently) HIPAA compliance trainings for all staff across the entire organization should be required. An organization must ensure that all employees have the most up to date knowledge and understanding of security concerns and procedures. Additionally, organizations must conduct Security Awareness Training and test employees through random synthetic testing while monitoring the results and assigning remedial training to those that fails to identify risks. In addition to regular trainings, a key practice to ensure continuous use is to distribute alerts to all employees when phishing attempts are reported. These alerts serve to both remind employees of their responsibilities and requirements under HIPAA and to keep them alert to the most cogent threats. These alerts are distributed as attempts are reported to IT, therefor they are regularly presented to employees throughout the year.

Another crucial method for ensuring security is in place is through the use of third-party auditing. The best test to ensure your cybersecurity infrastructure is in use and functioning as intended is to pay someone to attempt to foil it. Hiring trusted and vetted third party cybersecurity auditors to do what is called a vulnerability and penetration test, provides a great amount of detail to organizations regarding how effective their practices actually are and if they are implemented properly. In addition to ensuring proper implementation, these tests also allow a covered entity to become aware of any potential problems before bad actors notice and take advantage of vulnerabilities.

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

When defining a cybersecurity standard for organizations to utilize as their minimal requirement for the protection of sensitive data, the Department should look to other recognized sectors of industry and the frameworks they utilize like PCI-DSS, HITRUST, and SOC2 that have recognized certification criteria and require that audits be conducted annually to maintain accreditation. The number of organizations that do not conduct regular risk analysis in the healthcare industry is concerning and an accreditation requirement annually would offer great insight and information leading to securing the health data of patients.