February 8, 2019

Roger Severino
Director, Office for Civil Rights
200 Independence Ave, SW
Washington, DC 20201

Dear Mr. Severino:

The College of Healthcare Information Management Executives (CHIME), The Association for Executives in Healthcare Information Technology *(*AEHIT*),* and The Association for Executives in Healthcare Information Security *(*AEHIS*)* appreciate the opportunity to comment on the Office for Civil Rights' (OCR), "Request for Information on Modifying HIPAA Rules to Improve Coordinated Care," published in the *Federal Register* on December 14, 2018.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With more than 2,800 members, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate the effective use of information management to improve the health and healthcare in the communities they serve. Launched by CHIME in 2014, AEHIS represents more than 850 chief information security officers (CISOs) and provides education and networking for senior IT security leaders in healthcare. Also launched in 2014, AEHIT represents more than 500 senior IT leaders responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation.

We greatly appreciate that OCR is exploring possible changes to HIPAA rules which could improve the pathway to more coordinated care and the transition to value-based healthcare. In the RFI OCR seeks feedback on four areas: 1) Promoting Information Sharing for Treatment and Care Coordination; 2) Promoting Parental and Caregiver Involvement and Addressing the Opioid Crisis and Serious Mental Illness; 3) Accounting of Disclosures; and 4) Notice of Privacy Practices. OCR also asks for ideas on additional ways to remove regulatory burdens not otherwise addressed. CHIME's ideas are outlined below.

I. Key Recommendations

We make the following recommendations:

1. **Notice of Privacy Practices**: We recommend they only be required to be posted on an organization's website.

2. **Accounting of Disclosures (AOD)**: We appreciate that OCR has not finalized the 2011 proposed rule especially since AODs appear to be widely misunderstood, infrequently used, and often do not bring the intended value to the patient.
3. **Hybrid Entities**: OCR should create a safe harbor for hybrid entities like academic medical centers who have research components which allows these the provider to work with the research departments to share protected health information (PHI).
4. **Cloud Service providers (CSP)**: We recommend OCR clarify the CSP guidance and narrow the definition of a CSP that is considered a Business Associate such that they would only be one if they create, receive, maintain, or transmit electronic PHI (ePHI) and have access to an encryption key.
5. **Breaches**: We recommend OCR:
    a. Create a safe harbor for providers who have demonstrated they are meeting a set of best practices such as those developed under the public-private effort known as the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) (formerly referred to as 405d); and
    b. Make changes to Section 164 of CFR Title 45, *Notification in the Case of a Breach of Unsecured Protected Health Information*, as outlined further in our letter.

II. Responses to OCR Questions

A. Promoting Information Sharing for Treatment and Care Coordination

OCR is seeking feedback on whether changes to the right of access would support and promote care coordination and/or case management by enabling more timely transfer of PHI between covered entities, or between covered entities and other health care providers. The agency also seeks input on the scope of this problem, and on whether there are potential revisions to the Privacy Rule to support and promote care coordination and/or case management, including by requiring timely transfer of PHI for this purpose or other purposes, such as when a patient switches medical providers and their new provider requests the transfer of records from the previous provider.

OCR is also seeking feedback on whether changes to the right of access would support and promote care coordination and/or case management by enabling more timely transfer of PHI between covered entities, or between covered entities and other health care providers. The agency also seeks input on the scope of this problem, and on whether there are potential revisions to the Privacy Rule to support and promote care coordination and/or case management, including by requiring timely transfer of PHI for this purpose or other purposes, such as when a patient switches medical providers and their new provider requests the transfer of records from the previous provider.

Question #1: How long does it take for covered entities to provide an individual with a copy of their PHI when requested pursuant to the individual's right of access?

Response: In short, it depends on the complexity of the record. For instance, does it only relate to the EHR or the transaction record? Did the patient have a specific question? As one member noted, "It takes time if it's the record and not what is on the portal; it goes to the HIM department and it takes time to burn the CD and mail it out."

Question #2: How feasible is it for covered entities to provide PHI when requested by the individual pursuant to the right of access more rapidly than currently required under the rules?

Response: Our members find it feasible to provide PHI to patients under their right of access. We do believe there is some confusion, however, around how OCR's requirements and there is variability among providers in terms of how the requirements are being interpreted and met. It is our understanding that that when a patient requests their PHI pursuant to their right of access that this applies to the designated record set. Some providers, however, may be interpreting this to mean they must supply the entire EHR audit log.

Members report routinely being asked to produce EHR audit logs regarding whether a certain employee accessed a patient's record. One member said he receives these types of requests once or twice a week. While most of these instances do not entail handing over the entire audit log for these types of scenarios, when our members receive legal requests for the audit log the entire thing can be handed over for legal proceedings. Typically, our members are handing over what is in the designated record set. There does appear to be some confusion about what must be produced under the right of access.

Question #3: Should covered entities be required to provide copies of PHI maintained in an electronic record more rapidly than records maintained in other media when responding to an individual's request for access?

Response: Most members said this could be supplied within 5 days, but several other members felt they needed up to 30 days.

Question #4: What burdens would a shortened timeframe for responding to access requests place on covered entities?

Response: We worry about unintended consequences. Provider are being pushed to perform an increasing number of tasks electronically and to do so more quickly manner, yet we still do not have uniformity in standards for moving information which presents significant challenges for providers. We also worry that pushing things to happen too quickly electronically can result in mistakes being made. There are already several mandates in place for providers (i.e. Promoting Interoperability) to provide patients with information in less than 30 days. There is also the variance between state laws around release of information. Unless OCR preempts state laws, the baseline will remain state law.

Question #5b: Should health care clearinghouses be subject to the individual access requirements, thereby requiring health care clearinghouses to provide individuals with access to their PHI in a designated record set upon request?

Response: While many of our members indicated our members supported the ability for clearinghouses to provide patients with direct access to their PHI, we believe the answer to this question is more nuanced. Some of our members are very fearful that should clearinghouses be allowed to start offering patients access to their PHI that this could create more problems than it solves. One concern we have is that this becomes yet another independent data set that providers cannot control. As one member reflected, "The clearing house may very well have an incomplete record set and will create confusion for the patients. It will create issues for the providers that will have to respond to issues that fall out of a third party sharing data. There this is also the issue of positive patient identification, how will the clearinghouse ensure that they have provided the correct data sets."

Additionally concerning, we are aware that there is a legislative proposal concerning healthcare clearinghouses that would not only have eliminated the requirement for providers and payers to enter into Business Associate Agreements with clearinghouses, but also would have invalidated *existing* Business Associate Agreements between providers, payers and clearinghouses. Further, prior legislative proposals would have given clearinghouses special rights not afforded to other Covered Entities, such as granting clearinghouses a waiver from having to notify individuals directly in the event of a breach of unsecured PHI and the ability to charge individuals "fair market value" to respond to access requests.

Question #6: Do health care providers currently face barriers or delays when attempting to obtain PHI from covered entities for treatment purposes?

Response: Many of our members report experiencing barriers when attempting to get patient records from another provider which is a short answer to a complex question.

Question #7: Should covered entities be required to disclose PHI when requested by another covered entity for treatment purposes? Should the requirement extend to disclosures made for payment and/or health care *operations* purposes generally, or, alternatively, only for specific payment or health care operations purposes?

Response: Yes, covered entities should be required to disclosure PHI when requested by another covered entity when it pertains to treatment purposes.

Question # 9a: Currently, HIPAA covered entities are permitted, but not *required*, to disclose PHI to a health care provider who is not covered by HIPAA (*i.e.*, a health care provider that does not engage in electronic billing or other covered electronic transactions) for treatment and payment purposes of either the covered entity or the non-covered health care provider. **Should a HIPAA covered entity be required to disclose PHI to a non-covered health care provider with respect to any of the matters discussed in Questions 7 and 8?**

Response: Yes, however, some of our members cautioned that some other providers could be located outside the U.S. which could present risks.

Question #9c: Do the risks associated with disclosing PHI to health care providers not subject to HIPAA's privacy and security protections outweigh the benefit of sharing PHI among all of an individual's health care providers?

Response: Most of our members believe the risks of disclosing PHI to healthcare providers not subject to HIPAA do not outweigh the benefits.

Question #11: Should OCR create exceptions or limitations to a requirement for covered entities to disclose PHI to other health care providers (or other covered entities) upon request?

Response: We believe that providers need to be trusted to share only the information that is needed. Placing requirements on providers to seek consent to share PHI will erect barriers and burdens that in the end may impede needed sharing and patient care. Further, there could be situations where patients are unable to give consent.

Question #12: What timeliness requirement should be imposed on covered entities to disclose PHI that another covered entity requests for TPO purposes, or a non-covered health care provider requests for treatment or payment purposes?

Response: Our members varied in their opinions of what timeframes should be applied for sharing TPO with other covered entities. Many supported a timeframe of up to five days, while many others supported having up to 30 days. Our membership is diverse, and their abilities and needs vary, therefore, what may be entirely feasible for one provider may be much harder for another.

Question #13: Should individuals have a right to prevent certain disclosures of PHI that otherwise would be required for disclosure? For example, should an individual be able to restrict or "opt out" of certain types of required disclosures, such as for health care operations?

Response: No, individuals should not have the right to prevent certain disclosures of PHI that otherwise would be required for disclosure.

Question 14: How would a general requirement for covered health care providers (or all covered entities) to share PHI when requested by another covered health care provider (or other covered entity) interact with other laws, such as 42 CFR Part 2 or state laws that restrict the sharing of information?

Response: There are growing challenges faced by providers and their business associates as more information is exchanged electronically as they must navigate a complex regulatory and legal landscape. Providers must wrestle with myriad state laws coupled with the different consent policies associated with mental health and substance abuse rules under 42 CFR Part 2, making the electronic exchange of this

information very challenging. Complicating matters is segmenting sensitive data within EHRs remains very challenging. Further, use of application programming interfaces (APIs) during sensitive information exchange cannot be evaluated until the FHIR standards are available and API security challenges are addressed. For a more in depth discussion of APIs please see our letter to ONC on the EHR Reporting Program.

OCR Question #15: Should any new requirement imposed on covered health care providers (or all covered entities) to share PHI when requested by another covered health care provider (or other covered entity) require the requesting covered entity to get the explicit affirmative authorization of the patient before initiating the request, or should a covered entity be allowed to make the request based on the entity's professional judgment as to the best interest of the patient, based on the good faith of the entity, or some other standard?

Response: No, explicit permission from the patient should not be required to share PHI when requested by another covered entity. The professional judgement of the requesting entity should be enough.

OCR Question #16: What considerations should OCR take into account to ensure that a potential Privacy Rule requirement to disclose PHI is consistent with rulemaking by the Office of the National Coordinator for Health Information Technology (ONC) to prohibit "information blocking," as defined by the 21st Century Cures Act?

Response: Our members have raised four possible issues for consideration by OCR:

a) Since the time Continuity of Care Documents (CCDs) have begun being shared, some members have been challenged by patients who feel their privacy rights have been violated despite the sharing occurring under permissible circumstances. They question whether they would implicate data blocking rules (which have yet to be published) if they refused to share data with other providers. Also, how would this work in terms of meeting the Promoting Interoperability rules?
b) Variation in state privacy and consent laws are, in themselves, responsible for some level of information not being shared and at the very least it makes the electronic exchange of information more difficult.
c) Another issue which came up centers around opt-in vs opt-out states and providers which straddle both types of states. For instance, NY is an opt-in state whereas PA is opt-out. Providers which services both PA and NY run into these issues and have experienced challenges receiving records in a timely manner.
d) Finally, our members continue to experience electronic data sharing issues because of the lack of uniformly adopted standards for sharing, including the lack of a uniform way to uniquely identify patients which results from a Congressional ban on place since 1999. We consistently have advocated for the need for a single set of standards to be used when exchanging information electronically. Without this, providers are significantly burdened with costly interfaces. And, clinicians are burdened by having to cull thru data that is not well-organized creating challenges to

locate information needed to treat patients. For more information about the challenges faced by providers due to the lack of standards and other related burdens please see our recent letter to the Office of the National Coordinator for Health IT (ONC) here and our letter to ONC on the EHR Reporting Program.

Question 17: Should OCR expand the exceptions to the Privacy Rule's minimum necessary standard?

Response: Meeting the Minimum Necessary standard has been difficult for many of members. As one member noted, "You are either too far to the left or too far to the right" and it can become an inhibitor to sharing information. Some members cite challenges with logging who has accessed records and there has been confusion around who what precisely must be logged. In operationalizing these requirements, our members have identified as challenges implementing identity access control standards for medical devices; and uncertainty around access to drug treatment information.

Question 17a: For instance, should population-based case management and care coordination activities, claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development be excepted from the minimum necessary requirement?

Response: Today our members who are involved with alternate payment models struggle to get data in a timely manner. They believe there should be exceptions for care coordination and population health as this will facilitate participation in new models of care.

Question 17b: Would these exceptions promote care coordination and/or case management?

Response: Most of our members believe that exceptions to minimum necessary requirements related to population-based management would improve care coordination.

B. Promoting Parental and Caregiver Involvement and Addressing the Opioid Crisis and Serious Mental Illness

Question #22: What changes can be made to the Privacy Rule to help address the opioid epidemic?

Response: Many of our members report that people are afraid of openly sharing substance abuse information. Therefore, clinicians treating patients with a substance abuse disorder (SUD) may be totally unaware of the patient's medical history as it relates to their SUD.

When a provider is caring for a patient's health, it is essential that they have a complete medical history with all relevant information that will help them make clinical decisions to the best of their ability. To ensure the highest quality of care possible, information pertaining to substance use disorder (SUD) is pertinent. However, as it currently stands as required by 42 CFR Part 2, SUD treatment and diagnoses

are kept confidential from providers which can be extremely problematic when a clinician is attempting to treat someone but doesn't know their prior addiction history. Our members strongly support synchronizing these consent policies and reducing the burdens imposed by these two different sets of rules and facilitating consent for the purposes of treatment, payment and healthcare operations pursuant to HIPAA.

Question #24: Are there circumstances in which parents have been unable to gain access to their minor child's health information, especially where the child has substance use disorder (such as opioid use disorder) or mental health issues, because of HIPAA?

Response: Yes, our members are aware of situations when parents were unable to obtain access to their children's records. As examples, one member told us that both the emancipated minor and patient must sign release form with the health information management (HIM) department. Another member noted his hospital, like many others, disconnect parent access via the patient portal, to their minor children's records.

Question #25: Could changes to the Privacy Rule help ensure that parents are able to obtain the treatment information of their minor children, especially where the child has substance use disorder (including opioid use disorder) or mental health issues, or are existing permissions adequate?

Response: While the Privacy Rule allows a parent to have access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with State or other law, many states have laws prohibit this. In discussing this issue with our members and noting the complexities associated with parent access to their minor children's records, they noted that if parents are paying for their children's care that they would still receive the evidence of benefits (EOB) statements. Additionally, under the Affordable Care Act (ACA) children may remain on their parent's insurance until they are 26 years old. Therefore, if the care received by minors is to remain unknown to their parents, EOBs would need to be modified.

Question 25(b): Should any changes be made to specifically allow parents or spouses greater access to the treatment information of their children or spouses who have reached the age of majority?

Response: No, changes should not be made. The existing consent rules should be followed.

Question 25(c): Should changes be made to allow adult children to access the treatment records of their parents in certain circumstances, even where an adult child is not the parent's personal representative?

Response: No, changes should not be made; there is already a legal vehicle to obtain this. Adult children can seek to be appointed medical power of attorney.

Question #26: The Privacy Rule currently defers to state or other applicable law to determine the authority of a person, such as a parent or spouse, to act as a personal representative of an individual in making decisions related to their health care. **How should OCR reconcile any changes to a personal representative's authority under HIPAA with state laws that define the scope of parental or spousal authority for state law purposes?**

Response: Yes.

C. Accounting of Disclosures

OCR also seeks comment encouraging covered entities, particularly providers, to share treatment information with parents, loved ones, and caregivers of adults facing health emergencies, with a particular focus on the opioid crisis.

Question #27: How many requests for an accounting of disclosures do covered entities receive annually and from what percentage of total patients?

Response: In discussing this issue with our members, the request for a true AOD are very few. Examples from members we queried are below.

- One privacy officer we spoke with at an academic medical center which services 200,000 patients said his organization receives 12 a year and he thought this was on the high end. He noted once they tell them in a letter where their information has been disclosed, they are usually satisfied, and they don't hear much more beyond that.
- Other members reported:
    - 5 AOD requests out of 70,000 patients.
    - 1 or .000002%
    - 10-15

Patients will ask, however, for who touched or has seen their PHI and may request their entire record. What is often misunderstood by patients is they are not getting an accounting which involves treatment, payment or healthcare operations (TPO). The majority of requests, therefore, are not true AODs. For instance, many members report getting requests from patients about who snooped into their record.

We do believe there is confusion, however, around what a provider is required to release under an AOD and that more education from OCR would be helpful. Even among our members, it appears the understanding of what constitutes a true AOD is misunderstood. Additionally, there are some areas providers consider to be "grey" in terms of what constitutes healthcare operations such as registries and more clarity here would also be helpful. Also, not all patients understand that what they are receiving under an AOD is for disclosures outside of TPO.

Question 27a: Of these, how many requests specify a particular preferred electronic form or format, and to what extent do covered entities provide the accounting in the requested form or format?

Response: Our members report few patients ever specify a particular electronic format.

Question 28: How much time do covered entities take to respond to an individual's request for an accounting of disclosures?

Response: The time it takes appears to vary significantly among our members. It ranged from a few hours to other reporting this being very burdensome with more reporting this was time consuming. A few of the responses we received from members are below:

- "Days and it involves multiple systems."
- "If we would receive such a request – it would probably require 1 day of staff time, assuming there is a process in place in the EMR."
- "30 days"
- "We act as soon as possible, generally within a week."
- "This is very time consuming, depending on how long they have been a patient – in mental health this can be a very long time with many providers, case managers, residential
- Several reported it takes 2 weeks.

Again, it also appears that some members are confused by constitutes a true AOD.

Question 29e: How many such disclosures are made from EHRs?

Response: Our members varied significantly in their responses to this question ranging from those who said they have an EHR log to those said it varies and yet others said they it was hard to quantify.

Question 31: Should the Department require covered entities to account for their business associates' disclosures for TPO, or should a covered entity be allowed to refer an individual to its business associate(s) to obtain this information?

Response: No, covered entities should not be required to account for business associates' TPO disclosures.

Question 32a: For existing EHR systems: What would be the burden for covered entities to retain the information for three years?

Response: Our members believe retaining record for three years would be burdensome.

Question 32f: To what extent do covered entities maintain a single, centralized EHR system versus a decentralized system (*e.g.*, different departments maintain different EHR systems, and an accounting of disclosures for TPO would need to be tracked foreach system)?

Response: Slightly fewer than half of our members use multiple systems, and slightly more than half have a single EHR.

Question 39: If covered entities are unable to modify existing systems or processes to generate a full accounting of disclosures for TPO (e.g., because modification would be prohibitively costly), should OCR instead require covered entities to conduct and document a diligent investigation into disclosures of PHI upon receiving an individual's request for an accounting of disclosures for TPO?

Response: Our members had mixed opinions on this question with slightly more favoring OCR requiring covered entities to conduct and document a diligent investigation into disclosures of PHI upon receiving an individual's request for an AOD for TPO.

Question 43: What is the burden, in economic terms, for covered health care providers that have a direct treatment relationship with an individual to make a good faith effort to obtain an individual's written acknowledgment of receipt of the provider's NPP?

Response: Again, our members answers varied in response to this question. Several members indicated that patients do not appear to read the NPP. A sample of the response we received are below:

- "1. Hundreds of thousands of print images annually 2. Moderate amounts of electronic storage to maintain images of a signed document."
- "Very little if captured electronically."
- "No particular burden but it is one of so many consents and sheets a patient get that I certain no one reads them."
- "Minimal."
- "Millions in manpower and systems."

D. Notice of Privacy Practices

The Privacy Rule requires covered providers and health plans to develop a Notice of Privacy Practices (NPP) that describes individuals' heath information privacy rights and how their health information may be used and disclosed by the covered entity. OCR is seeking comments on whether they should eliminate or modify the requirement for covered health care providers to make a good faith effort to obtain individuals' written acknowledgment of receipt of providers' NPPs, to reduce burden and free up resources for covered entities to devote to coordinated care without compromising transparency or an individual's awareness of his or her rights.

Question 42c: How often, if at all, are covered health care providers required to have the patient sign updated versions of these forms (*e.g.*, annually, each visit, no subsequent updates required)?

Response: Our members varied in the frequency with which they required patients to sign updated NPPs ranging from each visit to no subsequent updates, and other varying timeframes.

Question 49a: What alternative methods might providers find useful to document that they provided the NPP?

Response: Ideas offered by our members included patient checklists, patient portals, tracking via a health information exchange, electronic consent, EHR checkbox. Some felt this should happen annually and posting to the website should be sufficient.

Question 50: What use, if any, do covered health care providers make of the signed NPP forms, or documentation of good faith efforts at securing written acknowledgments, that the Privacy Rule requires providers to maintain?

Response: Most members reported they did not do anything further with then NPP other than for legal purposes. A sample of the feedback we received is below:

- "None."
- "The document or data is stored in the HER. We haven't used it to date."
- "Litigation avoidance."
- "These are of no use."

E. Additional Ways to Remove Regulatory Obstacles and Reduce Regulatory Burdens to Facilitate Care Coordination and Promote Value-Base Health Care Transformation

Below, we have identified several areas where we think OCR could reduce burdens on providers while also smartly helping foster a climate which supports keeping patient information secure.

Breaches

The ever-increasing drive to a fully interoperable healthcare system and the ever-increasing amount of PHI which is digitized, creates a growing threat landscape for breaches. Even those providers with the maximum resources available, are challenged in warding off sophisticated attacks from criminal enterprises and nation states. Presently, there are several breach reporting and related requirements which are unduly burdensome for providers. If these issues are not addressed, they will perversely impact the move to value-based care by inhibiting information sharing. Several of the present-day requirements are unduly punitive and burdensome for providers. The current regulatory framework governing breaches presumes a breach has occurred unless a provider can demonstrate otherwise. This framework is problematic because:

- It lacks clear and practical guidelines for providers, and in practice results in substantial overreporting due to providers' confusion and their fear of repercussions.

- The extent of reporting has become so voluminous under the current framework that the regulation arguably renders the notification and reporting meaningless for patients, providers, government, and other stakeholders.
- Patients are likely unable to discern the instances breaches of information could result in personal harm. The information reported is so voluminous as to render it meaningless for patients and others interested in addressing real problems to protecting the privacy of patient records.
- The current HHS policy imposes a stigma on entities reporting a breach in perpetuity. The proposed changes seek a fair mechanism to relieve an entity of being listed as a "violator" once the entity takes action to correct its vulnerabilities.
- Finally, the proposed changes seek to strike a better balance between the protection of PHI, continuous and rapid evolution in technology including health technologies, and the practical realities of implementing privacy protections and practices.

Additionally, there is substantial confusion around what constitutes a breach. OCR, for instance, has determined that based upon the existing definition that all cyber incidents represent a breach. However, they are not necessarily reportable unless it is determined that PHI was compromised. OCR's ransomware guidance, for instance, is widely misunderstood and confusing for providers. Frequently PHI is not compromised but the fact that OCR constitutes it as a breach places an enormous burden on providers to prove PHI was not compromised.

Taking into account these concerns and the goals of the President's Executive Order 13771, which seeks to better manage regulatory burdens and costs associated with complying with federal regulations, we recommend

1. **Safe Harbor:** Proving a safe harbor for providers who have demonstrated they are meeting a set of best practices such as those developed under the public-private effort known as the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) (formerly referred to as 405d).
2. **CFR Title 45, *Notification in the Case of a Breach of Unsecured Protected Health Information*, Sections:**
    1. **164.402 (2) – Definitions:** The current one as construed implies guilt. We recommend amending this to reflect less the presumption of guilt and more clarity for entities to assess risk.
    2. **164.404 – Notification to Individuals**: We recommend amending the language around the responsibilities of business associates by adding that for breaches that start with them they must bear responsibility for subsections a-d.
    3. **164.406 (a) – Notification to Media:** We recommend adding language to ensure the BA is responsible for carrying out notifications when directed by CE.
    4. **164.408 – Notification to Secretary**: We recommend changes to ensure the BA is responsible for this as directed by CE AND add new language that indicates that posting information on HHS website will be limited to no longer than years or when corrective action plan is completed, whichever occurs first.

Cloud Service Providers

We also recommend OCR:

1. Make changes their Cloud Service provider (CSP) guidance that would clarify that the CSP is not a business associate either of a CE or BA; and
2. Narrow the definition of a CSP that is considered a BA; specifically, CSPs would be a Business Associate (either of the Covered Entity or as a subcontractor of a Business Associate) only if it creates, receives, maintains, or transmits ePHI and has access to an encryption key.

Hybrid Entities

We have received complaints from members working in academic medical centers pertaining to rules governing hybrid entities and the relationship to research departments. Specifically, research department that are pulled into an academic medical center's covered entity status and want to help with research activities are restrained under current rules around touching PHI. For example, a university's computer science department has the ability to do analytics work and would like to assist the health system, but the transfer of any PHI is not permitted under a Business Associate arrangement because the computer science department falls within the hybrid entity status and thus is ineligible to be a business associate.

We are:

1. **Seeking clarity from OCR around how research can occur under a hybrid entity relationship and they could you lose their hybrid entity status for engaging in work in which there is an exchange of PHI between the covered entity and non-covered entity; and**
2. **Requesting a safe harbor for hybrid entities engaging in these types of research activities which ultimately are being used to support patient care, especially given the increasing need for data analytics which are needed to support a value-based healthcare system.**

Conclusion

CHIME and AEHIS appreciate the opportunity to offer our feedback on this RFI and stand ready to have a longer dialogue on any of the topics discussed in our letter. Should you have any questions please contact Mari Savickis, vice president of federal affairs at msavickis@chimecentral.org.

Sincerely,

&

&

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Clint Perkinson
Director, Information Technology
Chair, AEHIT

Sean Murphy, VP & CISO, Premera
Chair, AEHIS