HIMSS
transforming health through information and technology™

33 West Monroe Street
Suite 1700
Chicago, IL 60603-5616 USA
Phone 312.664.HIMSS (664.4667)
Phone 312.664.6143
www.himss.org

February 12, 2019

Roger Severino, JD
Director, Office for Civil Rights
U.S. Department of Health & Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Mr. Severino:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), I am pleased to provide written comments to the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) in response to the Request for Information on Modifying HIPAA Rules To Improve Coordinated Care. I appreciate this opportunity to utilize our members' expertise in offering feedback on potential changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that would remove regulatory barriers to the sharing of protected health information (PHI) as a means to improve care coordination and interoperability, while ensuring the confidentiality, integrity, and availability of patient data.

As a mission-driven charitable organization, HIMSS offers a unique perspective with deep expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders, and influencers on best practices in health information and technology. Through our innovation companies, HIMSS delivers key insights, education, and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision.

As an association, HIMSS encompasses more than 76,000 individual members and 660 corporate members. We partner with hundreds of providers, academic institutions, and health services organizations on strategic initiatives to advance the use of innovative information and technology. Together, we work to improve health, access, as well as the quality and cost-effectiveness of healthcare. Headquartered in Chicago, Illinois, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, United Kingdom, the Middle East, and Asia Pacific.

Our healthcare system continues its shift toward value-based care, and it is critical that changes to HIPAA align with and build upon the broader healthcare transformation efforts that are being led by HHS. Throughout these Department-wide initiatives, the role of the patient is prioritized and their involvement in the control of their own data is key; targeting the appropriate resources to educate all parties on this model is a vital piece of our health system's evolution. We applaud OCR's work to evaluate regulations that may impede this transformation to value-based health

care or that limit or discourage coordinated care among individuals and covered entities, without meaningfully contributing to the protection of the confidentiality, integrity, and availability of individuals' PHI.

With these factors in mind, HIMSS offers the following overarching thoughts on potential changes to HIPAA:

- **It is imperative that HIPAA Regulations work in concert with the 21st Century Cures Act Information Blocking Rules**

As HHS moves forward with implementation of the 21st Century Cures Act (Public Law 114 - 255), the Department must ensure that any changes to the HIPAA Rules work in concert with the new rules around information blocking. The secure and ubiquitous exchange of health information is a significant undertaking for the entire community, and we want to be sure that the new rules around information blocking are clear and concise, and avoid any redundancies, conflicts, or inconsistencies with the HIPAA Rules which may result in confusion and impede progress. Ideally, the information blocking rules should encourage innovation and respect intellectual property rights, yet provide the right balance in regard to the sharing of information to enable care coordination, interoperability, and foster medical advancements and innovation.

HIMSS would like to keep HIPAA focused on articulating the standard ways that individuals' health information is to be used and disclosed. Our broader perspective on interoperability remains focused on ensuring the right people have the right access to the right health information at the right time. While we have made great strides over the past generation, seamless, secure, nationwide interoperable health information exchange continues to elude us. The HIMSS Call to Action: Achieve Nationwide, Ubiquitous, Secure Electronic Exchange of Health Information and HIMSS Cybersecurity Call to Action reinforce our commitment to these topics.

Many of the questions in the RFI ask about imposing requirements on various types of providers to share information, rather than simply permitting the provider to share information as needed. Our expectations are that the upcoming information blocking rules will help determine what information we have to share as well as how to enable the secure exchange and complete access of electronic health information without special effort on the part of the user. Given the impending rules on information blocking, HIPAA requirements in this area would be redundant and likely result in confusion. As such, we do not believe that HIPAA requirements in regard to information blocking is the appropriate vehicle to compel information to be shared with other healthcare stakeholders.

We encourage HHS to work internally to ensure HIPAA and the information blocking rules work in tandem and do not overlap or promulgate conflicting requirements. Many of the community-wide issues with HIPAA are focused on interpreting and sometimes over-interpreting what is allowable under HIPAA, so layering additional information blocking rules onto these processes will only add another source of burdens on clinicians and detract from the broader policy goals related to delivering better outcomes for patients. Overall, HIPAA alone cannot protect an individual's health information—and cannot facilitate or promote greater data sharing across the community; but HIPAA, in conjunction with sound information blocking rules, can be a significant step forward.

- **Any Changes to HIPAA Rules Should Prioritize the Needs and Role of the Patient in Care Coordination Activities**

HHS is moving forward on many fronts to empower patients with more control over their own data, and allow them to share their information with the provider of their choice. Under any changes in HIPAA rules, the patient must continue to be the primary authority in designating access to their data. In addition, organizations should not be able to share an individual's data for purposes other than treatment, payment, or health care operations without the expressed consent of that individual.

We envision that HIPAA should include a more explicit patient-centered consent framework that is straightforward for providers to administer and gives the patient the ability to share their data with another healthcare institution or a specific practitioner and also provides the patient the opportunity to segment some of their data for sharing for a particular period of time. Patients should have the means to identify care team members and data without originating provider knowledge or provider's affiliation with any care team. Under any scenario, the key principles are that the patient is involved, engaged, and at the center of any decision-making involving the sharing of their personal data.

For instance, at its core, the MyHealthEData Initiative from the Centers for Medicare & Medicaid Services (CMS) abides by the same principles. We would like to work with OCR to help design a new consent framework that capitalizes on these ideas and corresponds with the specifics of the information blocking rule and other regulatory measures.

As our healthcare delivery system continues to evolve toward even greater use of digital health tools, the functional paradigm around HIPAA must also progress. HIPAA will need to work in combination with the information blocking rules on determining the appropriate timeframes for responding to requests for patients' PHI. Requests for sharing PHI for the purposes of coordinating care are sometimes not fulfilled for 24-48 hours after they are made, and that has the potential to become a patient safety issue, particularly in exigent settings.

Digital health tools help reduce the barriers during care transitions, and improve the quality of those transitions. OCR should ensure that HIPAA rule updates take full advantage of these tools and prioritize the needs of patients. Improvements for patients in today's healthcare system rely on the patient being at the center of his or her care, which includes having access to data about their health, all while maintaining the confidentiality and integrity of that data.

- **Rule Modifications Should Ensure Alignment and Eliminate Regulatory Gaps Between HIPAA and State Laws as well as Other Measures**

HIPAA alignment with other laws and regulations is a key consideration when thinking about potential regulatory changes. The patchwork of existing state laws focused on health information privacy make for a challenging environment when attempting to share data. Most of these state laws are not preempted by HIPAA, so inter- as well as intra-jurisdictional information sharing is impacted by a myriad of regulation and uncertainty over what rules apply in particular circumstances. This has the potential to lead to hyper-interpretation as a means to achieve compliance as opposed to supporting the efficient sharing of key health information to advance high quality, valued-based care.

HHS published a report in June 2016 entitled, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*. It identified how large gaps in policies around access, security, and privacy continue, and confusion persists among both consumers and innovators. With new health-related technologies such as wearable fitness trackers, health social media, and mobile health apps gaining prominence in engaging patients, the report details how our laws and regulations have not kept pace with these new technologies. The HHS Report also identifies the lack of clear guidance around consumer access to, and privacy and security of, health information collected, shared, and used by those entities not covered by HIPAA. OCR should use this report as the foundation for making changes to HIPAA that minimize these regulatory gaps within the current statute.

HIMSS has also long advocated for changes to 42 CFR Part 2 (Part 2) requirements on the confidentiality of certain substance use disorder patient records to ensure alignment with HIPAA. The lack of clarity around the intersection of HIPAA and Part 2 places a significant burden on clinicians to interpret compliance with existing regulations. If clinicians had a clearer understanding of these regulations, including how they might intersect, they could improve care coordination, minimize a substantial source of burden, and allow appropriate access to patient information that is essential for providing whole-person care.

In addition, for global organizations, how HIPAA is reconciled with the European Union's new General Data Protection Regulation (GDPR) is another area where further guidance could be helpful to move closer to cross-jurisdiction and geographic alignment. As virtual care becomes more of the norm, and patients are able to exercise greater choice, this will become increasingly important. To ensure that HIPAA can remain relevant and adaptable, it is important to also consider future advances and changes to our healthcare delivery system when considering HIPAA modifications.

OCR has taken additional steps toward regulatory alignment with the withdrawal of the 2011 accounting of disclosures proposed rule following overwhelming community concerns about how existing, commonly used electronic health record (EHR) systems did not have the technical capability to produce the required access report and noting the necessary updates would be prohibitively costly for covered entities. HIMSS is encouraged by the steps OCR is taking to reengage the public on how individuals can obtain a meaningful accounting of disclosures that gives them confidence that their PHI is being disclosed appropriately as part of receiving coordinated care. Ensuring there is alignment between the HIPAA rules and the current marketplace's technological capabilities is a factor that should be included in any forward-looking evaluation.

Overall, HIMSS wants to synchronize and balance HIPAA privacy practices with the needs of our current electronic landscape, demands placed on the healthcare community by other laws and measures, and the strategic requirements of creating a learning healthcare system through better use and sharing of individuals' healthcare data.

- **HHS Must Redouble Efforts to Educate the Public and Providers About the Scope and Reach of HIPAA**

With an abundance of misinformation on how HIPAA should be implemented, and often hyper-interpretation of its rules given the complexity of the regulatory schemes and potential penalties for noncompliance, OCR should use this opportunity to institute more robust processes for

educating the public and providers about HIPAA privacy. Without additional education and much needed clarity, providers may withhold information or default to the most conservative course of action which, while protecting the provider from an enforcement action, does not benefit the patient or improve care coordination. Worse, it likely increases the total cost of care – both through the need to hire legal and compliance professionals to advise on the myriad of regulations as well as the missed opportunities to keep patients healthier.

Although OCR has created a process for individuals to file a complaint if he or she believes that a HIPAA-covered entity or its business associate violated their health information privacy rights or committed another violation of the Privacy, Security, or Breach Notification Rules, we encourage OCR perform significant outreach to the public so they understand their privacy rights under HIPAA. The campaign OCR began in 2018 with the Office of the National Coordinator for Health IT (ONC) that encourages individuals to get, check, and use copies of their health information is a positive step as is the work underway to offer training for healthcare providers about the HIPAA right of access.

OCR should also explore alignment with the new information blocking rules to set up a pathway for entities to jointly file complaints about other entities that are using HIPAA to block information. Such a campaign should include specific guidance on how to report potential violations as well as develop frequently asked questions (FAQs) about an individual's rights and responsibilities. Under the 21st Century Cures Act, ONC is tasked with creating a standardized process for the public to submit reports and claims of products failing interoperability or information blocking tests. As those rules are being developed, OCR should work with ONC to establish this process and include potential HIPAA violations as a part of their assessment.

In addition, we encourage OCR consider if this standardized process could provide an additional tool for an expedited review so that those entities claiming a HIPAA restriction on data sharing with another organization could have the opportunity for a swift challenge. There must be a clear-cut way for an individual or an entity to ask OCR to adjudicate these questions, and perhaps OCR could also explore the idea of creating incentives for providers to share information at the request of the patient, such as a situation where a provider would fall into a legal safe harbor if they compiled with such a request in good faith.

More emphasis from OCR on a community-wide HIPAA education protocol will play a significant role in empowering patients with the tools that they need to appropriately access and share their own data.

Based on the questions included in the RFI, we also offer the following comments:

> **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?**

HIMSS calls on OCR to ensure that any HIPAA requirements in this area work together with the upcoming information blocking rules and do not overlap or offer redundant requirements. Although such requirements would likely improve care coordination and case management, they do present opportunities for placing additional burdens on covered entities and individuals, so they must work in concert with information blocking. Additionally, as noted above, the greater the

complexity in the requirements the more likely it is that hyper-interpretation will ensue resulting in less care coordination and contributing to increased costs – thwarting the goal of supporting a shift to more high quality, value based care. HIMSS will continue to support robust privacy protections, but wants OCR to deliver clear guidance that encourages the safe portability of data through information blocking rules, HIPAA, as well as other measures.

> **9) 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? Would such a requirement create any unintended adverse consequences? For example, would a covered entity receiving the request want or need to set up a new administrative process to confirm the identity of the requester? 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?**

HIMSS endorses the idea that HIPAA covered entities should not be required to disclose PHI to a healthcare provider not also covered by HIPAA ("non-covered entity") that has not entered into an agreement to be bound by the equivalent protections and safeguards as mandated by HIPAA. HIPAA gives stakeholders certain levels of guarantees and safeguards required by the HIPAA Security Rule and the HIPAA Privacy Rule. HIPAA should never require any disclosure to another provider that is not obligated to provide for the same level of privacy protections and security measures as HIPAA, unless there is an agreement that has been entered into between the HIPAA covered entity and non-covered entity.

> **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? Should all covered entities be subject to the same timeliness requirement? For instance, should covered providers be required to disclose PHI to other covered providers within 30 days of receiving a request? Should covered providers and health plans be required to disclose PHI to each other within 30 days of receiving a request? Is there a more appropriate timeframe in which covered entities should disclose PHI for TPO purposes? Should electronic records and records in other media forms (e.g., paper) be subject to the same timeliness requirement? Should the same timeliness requirements apply to disclosures to non-covered health care providers when PHI is sought for the treatment or payment purposes of such health care providers?**

Working in concert with information blocking rules, HIPAA should refine timeliness requirements on use and disclosure of PHI by covered entities and ensure that relevant patient safety issues are appropriately addressed. Failure to fulfill requests for information sharing for 24-48 hours after such requests are made could potentially result in a patient safety issue, particularly in exigent settings. (Depending upon how critical the situation is, too, even 24-48 hours may be too long of a timeframe.) Digital health tools should help providers deliver more timely information on behalf of patients, but as most healthcare practitioners are already using EHRs, PACS, telemedicine, and other health IT tools, focusing the rules on the electronic exchange and portability of information

would help support the broader HHS work to implement an electronic-based, virtual healthcare delivery system.

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?

OCR cites instances of regulatory overlap and the rule redundancies that govern the information sharing issues that clinicians face every day. HIMSS recommends that OCR consider devising the HIPAA rules to further align with information blocking, state laws (such as those involving super protected health information), as well as the 42 CFR Part 2 rules. Alignment and education in these areas will help to further the needs of the patient, and reduce the burdens placed on clinicians to interpret multiple rules in the course of care delivery workflow. Further, such alignment would help improve patient care and coordination of such care. Presently, there are certain conditions, diagnoses, or treatments that a patient may have that is likely to be withheld from the covered entity, due to information barriers that result from state laws and the 42 CFR Part 2 rules. As a result, this could pose a serious risk to patient safety if, for example, a physician or a nurse is unaware of a patient taking a certain medication (e.g., for a mental health condition) that could adversely interact with another medication or treatment that the physician or nurse may give to the patient. (Indeed, drug-drug and drug-allergy interactions are quite possible and could potentially render serious adverse health effects.)

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?

HIMSS recommends that all federal programs and regulations focused on healthcare information sharing should be fully aligned with HIPAA to ensure that the simultaneous layering of all of these rules does not create extra burden on or increase costs for patients or covered entities when creating, receiving, maintaining, or transmitting PHI.

17) Should OCR expand the exceptions to the Privacy Rule's minimum necessary standard? 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? Would these exceptions promote care coordination and/or case management? If so, how? Are there additional exceptions to the minimum necessary standard that OCR should consider?

HIMSS supports the idea of minimum necessary requirements as a means to protect and secure PHI, however, as our health system continues to move toward greater use of populations-based case management and use of alternative payment models (APMs), clinician information needs to support transitions of care as well as better overall coordination of care only increase. As our healthcare system continues to shift from volume-based to value-based care delivery, we envision a system that utilizes health information and technology to drive to that future state where patients receive higher quality, safer, and more efficient care and clinicians can focus on patient safety and achieving better outcomes.

We encourage OCR to work with ONC and the Centers for Medicare & Medicaid Services (CMS) to further define the minimum necessary requirements to promote the shift to value-based care and satisfy the information needs of clinicians functioning under this new paradigm. Guidelines or examples on what may meet the minimum necessary requirements would be helpful to the community as it moves forward. However, having specific "one size fits all" minimum necessary rules could block or filter out important information needed for use by care managers during transitions of care or caregivers in the delivery of care to the patient. Having incomplete information could end up being a significant patient safety issue. In essence, the minimum necessary requirements should ensure that covered entities have, at minimum, the essential elements of information necessary to effectively provide high quality care and care coordination by providing the right information at the right time for the right patient to the appropriate caregivers and/or care managers.

Additionally, OCR should better define the minimum necessary standards so that clinicians could receive a complete and accurate description of the patient's condition during transitions of care. We recommend that OCR look to the CMS Data Element Library as a source to help better define the minimum necessary standard. The Data Element Library promotes interoperable health information exchange by linking CMS assessment questions and response options to nationally accepted health IT standards. CMS emphasizes that standardized and interoperable data support health information exchange across healthcare settings to facilitate care coordination, improved health outcomes, and reduced provider burden through the reuse of appropriate healthcare data.

In addition, OCR can also look to the ONC's draft Trusted Exchange Framework and Common Agreement, (TEFCA), and the accompanying US Core Data for Interoperability (USCDI), which specifies a common set of data classes that are required for interoperable exchange and identifying a predictable, transparent, and collaborative process for achieving those goals. As ONC moves forward with development of the second iteration of TEFCA and USCDI, OCR should look for opportunities to leverage those tools in discussions around the minimum necessary standards.

> **18) Should OCR modify the Privacy Rule to clarify the scope of covered entities' ability to disclose PHI to social services agencies and community-based support programs where necessary to facilitate treatment and coordination of care with the provision of other services to the individual? For example, if a disabled individual needs housing near a specific health care provider to facilitate their health care needs, to what extent should the Privacy Rule permit a covered entity to disclose PHI to an agency that arranges for such housing? What limitations should apply to such disclosures? For example, should this permission apply only where the social service agency itself provides health care products or services? In order to make such disclosures to social service agencies (or other organizations providing such social services), should covered entities be required to enter into agreements with such entities that contain provisions similar to the provisions in business associate agreements?**

HIMSS endorses the idea that HIPAA covered entities should not be required to disclose PHI to a social service agency not also covered by HIPAA ("non-covered entity") that has not entered into an agreement to be bound by the equivalent protections and safeguards as mandated by HIPAA. HIPAA gives stakeholders certain levels of guarantees and safeguards required by the HIPAA Security Rule and the HIPAA Privacy Rule. HIPAA should never require any disclosure to a social service agency that is not obligated to provide for the same level of privacy protections and security

measures as HIPAA, unless there is an agreement that has been entered into between the HIPAA covered entity and non-covered entity.

Overall, HIMSS is very supportive of collecting social determinant of health (SDOH) data and incorporating that information into the clinician workflow to benefit patients, but any sharing of related SDOH data needs to rely on the same guarantees and safeguards inherent in the HIPAA Rules or the equivalent protections thereof (e.g., as set forth in a written agreement).

20) Would increased public outreach and education on existing provisions of the HIPAA Privacy Rule that permit uses and disclosures of PHI for care coordination and/or case management, without regulatory change, be sufficient to effectively facilitate these activities? If so, what form should such outreach and education take and to what audience(s) should it be directed?

Public outreach and additional education for patients, caregivers, the provider community, and their business associates are critical for the continued success of the HIPAA Privacy Rule. Educational efforts should be targeted at all levels of the care continuum—from providers to their non-clinician office staff and business associates, along with patients, so that all parties understand the requirements as well as the gaps in the existing rules. HIMSS is open to working with OCR to convene patient advocacy groups and health IT organizations to pursue as many avenues as possible to assist in this meaningful education of all healthcare system stakeholders.

22) What changes can be made to the Privacy Rule to help address the opioid epidemic? What risks are associated with these changes? For example, is there concern that encouraging more sharing of PHI in these circumstances may discourage individuals from seeking needed health care services? Also is there concern that encouraging more sharing of PHI may interfere with individuals' ability to direct and manage their own care? How should OCR balance the risk and the benefit?

The further alignment of HIPAA, 42 CFR Part 2 rules, and state laws would help to address the opioid crisis. Providers need to have a clear sense of what information can be shared, with whom, and not be hindered in their information sharing efforts by uncertainty over what rules apply in particular circumstances and potential over-interpretation of the rules.

In addition, HIMSS has expressed strong support for the overall role of greater information sharing to combat the opioid crisis and contribute to a reduction in the risks associated with implementing such changes. HIMSS is fully supportive of efforts to improve interoperability between EHRs and state prescription drug monitoring programs (PDMPs) as well as increasing adoption of electronic prescribing of controlled substances (EPCS). Each of these concepts are implemented at the state level, so the patchwork of state laws we describe plays a factor in how well data is exchanged and the controls that are in place over opioid-related information.

Moreover, the role of the patient is paramount in helping to address the crisis. Under our care delivery model, the patient should control access, movement, participants, length of time, and breadth of access to their information. At different points in the care continuum, various providers may each need access to some or all information to provide the best care to the patient, as the patient desires, for a time period the patient designates, and to be shared with informed consent. Providing more educational opportunities to individuals about the safeguards in place through HIPAA could provide them the peace of mind for sharing their information and increase their

comfort level with seeking treatment by alleviating their concerns about the confidentiality of their health information.

41) The HITECH Act section 13405(c) only requires the accounting of disclosures for TPO to include disclosures through an EHR. In its rulemaking, should OCR likewise limit the right to obtain an accounting of disclosures for TPO to PHI maintained in, or disclosed through, an EHR? Why or why not? What are the benefits and drawbacks of including TPO disclosures made through paper records or made by some other means such as orally? Would differential treatment between PHI maintained in other media and PHI maintained electronically in EHRs (where only EHR related accounting of disclosures would be required) disincentivize the adoption of, or the conversion to, EHRs?

HIMSS emphasizes that accounting of disclosures often entails the collection of volumes of pages that are typically not useful to the requester. In addition, production of the accounting of disclosures is time-consuming, very labor-intensive, costly, and can take up to 24 hours, or more, to produce. This information is normally maintained in electronic format and if OCR were to consider adding disclosures made through paper records or by other means, it would only broaden the burdens placed on providers in these instances. Given our health system's intentional move toward more digital health tools, we encourage OCR to limit the scope of accounting of disclosures to PHI maintained electronically in EHRs or other electronic health information systems wherein the retrieval of such information would be relatively seamless and automatic (e.g., using structured data sets).

We also recommend that the reason for the disclosure needs to be part of the designated record set as it is a major task to produce an accounting of disclosures. Due to the huge volume of available data, the requester's questions are usually not easily answered. Overall, the return on investment is quite low for this entire process, and that should be acknowledged through any changes to the HIPAA rules.

We also endorse the use of ASTM International's Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems (ASTM E2147 – 18) for the data elements that should be provided in an accounting of treatment, payment, or health care operations disclosure. This specification details how to design an access audit log to record all access to patient identifiable information maintained in computer systems, and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of confidential health care information to external users for use in manual and computer systems.

51) What benefits or adverse consequences may result if OCR removes the requirement for a covered health care provider that has a direct treatment relationship with an individual to make a good faith effort to obtain an individual's written acknowledgment of the receipt of the provider's Notice of Privacy Practices (NPP)? Please specify whether identified benefits or adverse consequences would accrue to individuals or covered providers.

A signed acknowledgement of an NPP can be burdensome to obtain, and it may be difficult to obtain/require follow-up care if a patient is unable to sign upon the initial encounter. The NPP is typically an additional form packaged along with admission or other required documentation

that a patient must sign. Overall, it adds little value as most individuals don't have the meaningful opportunity to review the NPP prior to having to sign the acknowledgement. HIMSS recommends that NPPs continue to be required to be prominently posted in service areas, and on the covered entity's website. An option for OCR to consider implementing in this area is to attempt to track internally that the NPP was offered or provided to individuals for their review, but not require the individual's signature.

54) In addition to the specific topics identified above, OCR welcomes additional recommendations for how the Department could amend the HIPAA Rules to further reduce burden and promote coordinated care.

The breach notification rule, as presently implemented, requires covered entities to report breaches of unsecured PHI, even if the origin of the breach is the business associate. Business associates are only under the obligation to notify the covered entity of the breach. Unfortunately, this places an undue burden on the covered entity and also causes reputational damage - despite that the covered entity may have attempted to comply with all requirements, including implementation of a business associate agreement. When considering HIPAA rule changes, HIMSS recommends that HHS re-evaluate the breach notification rule, including its impact, when considering a final rule, and consider other approaches for the reporting of breaches.

HIMSS is committed to be being a valuable resource to HHS and OCR, along with the entire healthcare community, to make sure patient data remains secure while finding ways to remove regulatory barriers in the sharing of PHI.

We welcome the opportunity to meet with you and your team to discuss our comments in more depth. Please do not hesitate to contact Jeff Coughlin, Senior Director, Federal & State Affairs, at 703.562.8824, or Eli Fleet, Director, Federal Affairs, at 703.562.8834, with questions or for more information.

Thank you for your consideration.

Sincerely,

Harold F. Wolf III, FHIMSS
President & CEO
HIMSS