American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

February 12, 2019

Roger Severino
Director, Office for Civil Rights
U.S. Department of Health and Human Services
Attention: RFI, RIN 0945-AA00
Humbert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Re: Request for Information on Modifying HIPAA Rules to Improve Coordinated Care (RIN 0945-AA00)

Dear Director Severino:

On behalf of the nearly 5,000 member hospitals, health systems and other health care organizations, and our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to comment on the request for information (RFI) on modifying Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules to improve coordinated care.

America's hospitals and health systems are dedicated to safeguarding the privacy of patients' medical information. The AHA and its members believe that the current HIPAA rules generally offer an effective framework that permits covered entities, like hospitals and other health care providers, to share patients' protected health information (PHI) for the purposes of treatment, payment and health care operations without creating significant impediments to the robust use and disclosure of patients' PHI necessary to support high-quality care, care coordination and population health improvement.

We support efforts to decrease regulatory burdens for covered entities and remove unnecessary barriers that prevent or inhibit efficient care coordination and/or case management and do not further the transformation to value-based health care that simultaneously also respect and preserve the privacy and security of patients' health information. However, we believe that many of the concerns related to barriers and obstacles to sharing information the RFI's questions raise would be best addressed through guidance and education. Frequently, it is the lack of such guidance from the Office for Civil Rights (OCR) that does more than repeat the language of the regulatory text that can create anxieties among covered entity providers about potential noncompliance and its significant consequences that leads them to be extremely cautious about using and disclosing patients' information for efficient care coordination and/or case management and to advance value-based health care. When unsure, the default position is to not disclose or share patients' information unless and until individual patient authorization has been secured.

However, because HIPAA currently does not preempt other federal or state laws that require patient information be treated and handled differently, a prime example of which is the Part 2 statute and regulation discussed further below, the resulting patchwork of health information privacy requirements remain a significant barrier to the robust sharing of patient information necessary for coordinated clinical treatment, improving the quality of care and maintaining population health. In addition, the patchwork of differing requirements poses significant challenges for providers' use of a common electronic health record (EHR) that is a critical part of the infrastructure necessary for effectively coordinating patient care and maintaining population health.

The AHA has long advocated that the HIPAA requirements be the prevailing nationwide standard for protecting the privacy and security of all patient information. **The AHA affirms its support for full federal preemption under HIPAA.** While we recognize that reform of the preemption framework likely may require involvement of the legislative branch, we urge OCR to prioritize efforts aimed at educating Congress about the significant burdens the lack of preemption imposes for robust information sharing necessary for effective care coordination and/or case management and the transformation to value-based health care.

Promoting Information Sharing for Treatment and Care Coordination

Hospitals and health care providers want to share health information to support care coordination, case management and the transition to value-based health care and do so when permitted legally. **Amending the privacy rules to require covered entities to disclose PHI to other covered entities will not promote greater information sharing for these important purposes.**

The HIPAA rules currently limit the sharing of a patient's medical information for "health care operations" like quality assessment and improvement activities, including outcomes evaluation, or activities related to the evaluation of provider qualifications, competence or performance, to information about those patients for whom both the disclosing and receiving providers have – or have had – a patient relationship. The challenge that this regulatory prohibition poses in the new environment of value-based care and for integrated care settings is that patients frequently do not have a direct care relationship with all of the providers among whom information should be shared and coordinated. But in a clinically integrated setting, each of its participating providers must focus on and be accountable for all patients. Moreover, achieving the meaningful quality and efficiency improvements that a clinically integrated setting promises requires that all participating providers be able to share and conduct population-based data analyses.

The HIPAA medical privacy regulation should permit a patient's medical information to be used by and disclosed to all participant providers in an integrated care setting without requiring that individual patients have a direct treatment relationship with all of the organizations and providers that technically "use" and have access to the data.

The AHA supports keeping the privacy rule's existing timeliness requirements for responding to requests for access unchanged. These requirements, which mandate that covered entities must act on a request for access no later than 30 days after receiving the request and provides for only one 30-day extension of time to act on access request (provided that the covered entity provides a written statement of the reasons for the delay and the date by which it will complete any action on the request), are outer limits. Maintaining the current approach is preferable to amending the rule to impose different timeliness standards based on the manner in which the PHI is maintained.

Covered entities current practice is to respond promptly to requests. Moreover, OCR has been clear that waiting the entire 30 days to provide access may be a violation of the HIPAA requirement in some circumstances. In addition, state and other legal requirements, including requirements related to EHR meaningful use, already have eclipsed the specific HIPAA requirements, eliminating the need to revise the HIPAA rules to establish different timeliness standards. The different timeliness standards currently applicable through state and other federal laws are themselves complicated and burdensome to administer.

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

The HIPAA privacy rule currently recognizes the integral role that family, friends and others, including multi-disciplinary/multi-agency health and social service teams, play in a patient's health care and in addressing the social determinants that impact the patient's health. Permissible use and disclosure of patient information include health care providers' communications with a patient's family, friends, or other persons who are involved in the patient's treatment and care, provided those communications are limited to only the PHI directly relevant to the person's involvement in the patient's care or payment for care. Increasingly, permissible communications necessarily must include communications with social service agencies helping to address social determinants affecting the patient's health. **Better, more detailed guidance that helps providers understand the broad scope of such permissible uses and disclosures would promote greater parental and caregiver involvement in responding to the opioid crisis and serious mental illness. It also would encourage greater information sharing for care coordination and/or case management and the move to value-based care delivery.**

Likewise, the minimum necessary requirement ─ mandating that HIPAA covered entities make "reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request" ─ has been treated as a "reasonableness standard," not an "absolute standard" since its inception. Time and again, OCR has confirmed that covered entities have "substantial discretion with respect to how [they] implement the minimum necessary standard." These OCR statements provide some continuing comfort to hospitals and other covered providers that the minimum necessary requirements need not impede the provision of quality care and services, and that minimum necessary determinations by providers will be judged under a standard of reasonableness. We believe that this approach to the minimum necessary requirement remains vitally important for care coordination and effective case management and the transformation to value-based care. **OCR could give provider covered entities greater confidence that they are acting in compliance with their minimum necessary obligations when sharing a patient's information with the patient's family, friends, or other persons who are involved in the patient's treatment and care and for care coordination and/or case management by simply establishing a safe harbor respecting the treating provider's judgment about minimum necessary.**

The AHA also urges full alignment of the Part 2 regulation with the HIPAA regulation as the proper and effective solution to eliminating the existing barriers to the sharing of patient information essential for care coordination, compatible with electronic exchange of information and supportive of performance measurement and improvement. Applying the same requirements to all patient information − whether behavioral- or medically-related − would support the appropriate information sharing essential for clinical care coordination and population health improvement in today's patient care environment, where behavioral and medical health care are integrated to produce the best outcomes for all patients.

The separate privacy structure under 42 CFR Part 2 creates challenges for the integration of behavioral and physical health care simply because patient data related to behavioral health cannot be handled like all other health care data. Estimates are that one in four Americans experiences a behavioral illness or substance use disorder each year, and the majority of these individuals have a comorbid physical health condition. Moreover, primary care has become the prevailing location for patients to receive treatment that addresses all their health needs – behavioral as well as medical. Evidence confirms that integrating mental health, substance use disorder and primary care services produces the best outcomes and proves the most effective approach to caring for people with multiple health care needs.

Furthermore, at the highest stage of care integration, the focus is not merely on improving medical outcomes for individual patients but managing population health while reducing total costs for the overall health care delivery system. To meet the needs of the many individuals with complex health needs, however, providers must be able to share patient behavioral health information as easily as information related to physical health for purposes of treatment, payment and health care operations, (i.e., without having to obtain each individual patient's authorization as HIPAA permits).

The requirement in the Part 2 regulation for individual patient consents to make sharing of behavioral health information permissible seems to overemphasize the social harms that disclosing such clinical information is perceived to create at the risk of medical harms and overdose deaths that are a consequence of poor coordination of care for such patients. Moreover, because the requirement to obtain individual patient consents significantly complicates the sharing of important patient information essential for coordinating care and population health improvement, it contributes to higher health care costs for patients with complex health needs, who already are among the highest-cost utilizers in health care. Permitting providers to handle and treat patient data related to behavioral health as simply another part of a patient's health care data protected by HIPAA is a critical component of a demonstrated more effective approach to caring for and achieving the best outcomes for all patients.

While we recognize that reform of the underlying statute remains the purview of the legislative branch, we urge OCR to work with the Substance Abuse and Mental Health Services Administration (SAMHSA) to prioritize efforts aimed at educating Congress about the significant burdens the existing statutory framework imposes for the integration of behavioral health and other medical care and the transformation of care delivery to value-based and population health system. A combined effort directly by OCR and SAMHSA would do much to facilitate the sharing of information necessary for coordinated care delivery and improved health outcomes for all patients than the nominal revisions of the Part 2 regulation itself.

Earlier revisions to the regulations generally maintain the status quo of requiring individual patient consents for disclosure and thereby compels health care providers to maintain a strict separation of a patient's behavioral health-related data from other patient data. In addition, the revised relation retain an overly broad applicability to treatment programs and providers in the definition of the regulation's applicable scope. While SAMHSA carved out general medical facilities and medical practices from the scope of the Part 2 regulation in what at first seems a broad general carve out, the agency immediately restricts that carve out in the definition. Specifically, general facilities and practices are excluded from the scope of the Part 2 regulation, and thereby from complying with the significant regulatory constraints imposed on sharing a patient's behavioral health data, *only if* they do not hold themselves out as providing substance use disorder diagnosis, treatment or referral for treatment and the primary function of their medical personnel or other staff is not the provision of, and they are not identified as providing, such services.

In the current care environment, where there is expanding emphasis on integration and coordination of behavioral health care with physical health care and where the prevailing location for delivery of that care is the general medical facility or medical practice, SAMHSA, by doing do, effectively reduces the regulation's flexibility for sharing patient information. That is because the severe constraints and significant burdens on sharing a patient's behavioral health information the regulation imposes are likely to be seen by providers as applying to many more treatment settings and providers. This is particularly true because SAMHSA offers no detailed guidance about how providers are to determine whether they are “holding themselves out,” or whether the “primary function of their medical personnel or other staff is the provision of and they are identified as providing” the enumerated services. **We also urge OCR to work directly with SAMHSA to assist in further revision of the Part 2 regulation to create greater alignment with the HIPAA requirements that govern all other patient health information.**

Accounting of Disclosures

The AHA supports OCR’s withdrawal of its previous proposal to establish an individual right to an access report. The proposal for an access report was misguided. It did not appropriately balance the relevant privacy interests of individuals with the substantial burdens on covered entities, including hospitals, as the Health Information Technology for Economic and Clinical Health Act (HITECH) statute requires. It also was based on a fundamental misunderstanding of the value to individuals of receiving the particular information that the access report would capture, as well as a misunderstanding about the capabilities of technologies available to and used by covered entities to capture such information.

There already are a number of ways in which patients are informed about how their information is used and disclosed by a covered entity. For example, patients receive a hospital’s Notice of Privacy Practices, which includes not only a general description of the types of uses and disclosures for treatment, payment and health care operations, but also specific examples of each type of use and disclosure. Importantly, the notice also contains information about how individuals can communicate with a covered entity if they believe their information may be at risk of misuse or their privacy rights have been violated. The experiences of hospitals to date suggest that patients are more interested in knowing whether a specific violation relating to their electronic medical record has occurred and getting detailed information in response to a specific inquiry and investigation by the hospital’s privacy and compliance staff. Patients value these investigations because they provide information about specific violations and what appropriate disciplinary and other measures were taken to ensure that violations do not reoccur. A patient concerned about a future potential misuse, such as a relative working in the hospital who may inappropriately access records, also can use this mechanism to work with a hospital in advance to create a process for minimizing the possibility that such inappropriate access will occur. These processes and practices already are in place and are aimed to ensuring that patients are getting the information they feel they need and most value. **The AHA believes that an additional regulatory mandate to investigate a patient’s privacy concerns, especially one establishing a one-size-fits-all investigatory process, is unnecessary.**

The AHA appreciates that in the previously issued proposed rule that would have established the right to an access report, OCR identified some specific exclusions to the existing HIPAA accounting of disclosures requirements and noted that these exclusions preserved the value of the accounting of disclosures right for individuals, while limiting the burdens to covered entities. The AHA agrees with that view and would hope that

OCR would finalize these exclusions to alleviate regulatory burdens for covered entities' current compliance, including:

- Impermissible disclosures where a covered entity has provided a breach notification;
- Disclosures to report child abuse or neglect as well as disclosures related to reports of adult abuse, neglect or domestic violence;
- Disclosures for military and veterans' activities, Department of State medical suitability determinations, government programs providing public benefits;
- Disclosures required by law;
- Disclosures for research where an institutional review board (IRB) or privacy board has made a determination that the privacy interests of individuals are properly taken into consideration;
- Disclosures for health oversight activities; and
- Disclosures about decedents made to coroners, medical examiners and funeral directors, as well as disclosures for purposes of cadaveric organ, eye or tissue donation.

The AHA also supports limiting the accounting requirement to three years. We believe this will limit the burdens on covered entities without meaningfully limiting individual privacy interests, providing an appropriate balance of the burdens and benefits.

In addition, the AHA supports continuing to exclude from the accounting obligation disclosures:

- To individuals of their own PHI;
- Incident to an otherwise permitted or required disclosure;
- Pursuant to an individual's authorization;
- For the facility directory or to persons involved in the individual's care or other notification purposes;
- For national security or intelligence purposes;
- To correctional institutions or in law enforcement custodial situations; and
- As part of a limited data set.

These exclusions are consistent with maintaining a balance between individual privacy interests and the burden on covered entities in implementing the privacy requirements. These exclusions also are appropriate given the legal circumstances of the exclusions (i.e., national security purposes), with the concept that an accounting should not be required where an individual likely is aware of the disclosure (i.e., disclosures pursuant to an authorization), or that would unduly impede health care activities (i.e., disclosures incident to a permissible disclosure).

Notice of Privacy Practices

The AHA supports the elimination of the requirement for covered health care providers to make a good faith effort to obtain individuals' written acknowledgment of receipt of providers' Notice of Privacy Practices. We agree with OCR's assessment that the elimination of the requirement would 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.

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

In light of business associates' direct HIPAA compliance obligations under the HITECH Act and the related final rule, we believe that OCR should consider whether it remains necessary to require covered entities to enter into business associate agreements that include detailed provisions obligating business associates' compliance with regulatory requirements that are directly applicable to them. The application of business associate obligations directly to business associates through the text of the HIPAA privacy and security rules provide greater clarity and awareness of applicable regulatory requirements and thereby facilitate better compliance. It also would allow covered entities to focus contractual negotiations on the business purpose necessitating the relationship and would minimize the need to continually revise and negotiate business associate agreements following changes in the law and regulations.

Despite complying with HIPAA rules and implementing best practices, hospitals and health care providers will continue to be the targets of sophisticated cyber attacks, and some attacks will inevitably succeed. Whether exploiting previously unknown vulnerabilities or taking advantage of an organization with limited resources, attackers will continue to be successful. **The AHA believes that victims of attacks should be given support and resources, and enforcement efforts should rightly focus on investigating and prosecuting the attackers.**

Merely because an organization was the victim of a cyber attack does not mean that the organization itself was in any way at fault or unprepared. Similarly, a breach does not necessarily equate to a HIPAA security rule compliance failure. Moreover, an aggressive regulatory enforcement approach could be counter-productive and hinder valued cooperation by the victims of cyber attack with other parts of the government, such as the Department of Homeland Security (DHS), FBI and the intelligence community. Instead, successful attacks should be fully investigated, and the lessons learned should be disseminated widely to prevent successful similar future attacks.

In addition, we urge OCR to consider ways to develop a safe-harbor for HIPAA-covered entities that have shown, perhaps through a certification process, that they are in compliance with best practices in cybersecurity, such as those promulgated by HHS, in cooperation with the private sector, under section 405(d) of the Cybersecurity Information Share Act. Those best practices were developed through broad public-private collaboration after months of deliberation and development. A safe harbor would give covered entities clarity about the level of diligence they need to exercise, including when they agree to share and exchange PHI with other systems/organizations through tools like health information exchanges, to avoid OCR enforcement when an attacker gains access.

Since the passage of HIPAA in 1996, patients have understood that HIPAA-covered entities keep patients' health information confidential and secure, and hospitals and health systems continue to use and disclose patients' health information in accordance with the very exacting requirements of the HIPAA rules that include obligations to comply with more restrictive state and other federal privacy laws. However, these same exacting requirements do not apply to non-HIPAA covered entities that have different – and possibly in direct conflict with the HIPAA obligations of covered entities – responsibilities for information sharing and respecting patients' privacy and security. This uneven playing field raises concerns for HIPAA-covered entity providers in relation to proposals that would require broad and open free exchange of patient information with app developers or penalize information blocking.

Commercial app companies generally are not HIPAA-covered entities. Therefore, when information flows from a hospital's information system to an app, it likely no longer will be protected by HIPAA. Patients will not be aware of this change and may be surprised when commercial app companies share their sensitive health information obtained from a hospital, such as diagnoses, medications or test results, in ways that are not allowed by HIPAA. Furthermore, patients may consider the hospital to be responsible if their data – that may be indistinguishable from that held by the hospital – is sold to a third party or used for marketing or other purposes.

While we understand that patients have the right to share their data as they see fit, and may be willing to take the risk of less privacy when using commercial apps, we believe that significant consumer education efforts are needed to help individuals understand the vastly different, and less stringent, federal privacy requirements for entities not covered by HIPAA. **Therefore, to address concerns about patient privacy, we urge OCR to work with the Centers for Medicare & Medicaid Services (CMS), the Office of the National Coordinator for Health Information Technology (ONC) and the Federal Trade Commission (FTC), which enforces consumer protection, to provide model language that health care providers could use with their patients that choose to access their data via an app.** This language should clearly explain that data shared with and held by the commercial app is no longer protected by HIPAA, but is governed by the privacy policy and terms of service of the commercial app company. The language also should make clear that the health care provider bears no responsibility for the use of patient data by the commercial app company and that any concerns about how data are used once shared with an app should be directed to the FTC.

We also strongly recommend that OCR work with other agencies to develop an extensive education program so that all consumers can become aware of how app companies can and may use their data, and the importance of reviewing and keeping updated about the privacy practices of any app that they choose to use to access their sensitive health information.

ONC currently is developing rules and guidance to support information exchange and enforce the statutory prohibition on information blocking in the 21st Century Cures act. **The AHA urges OCR to work with ONC to ensure that the obligations of HIPAA-covered entities are adequately considered when these rules and guidance are developed.** For example, we have concerns about overly broad information sharing and blocking proposals that would permit the failure by HIPAA-covered entities to respond to any request for information to be reported and penalized as a possible instance of information blocking. HIPAA-covered entities may not be able to respond to a particular query if there is insufficient information to determine whether information can be shared, or if the request cannot be filled due to the other limitations imposed by HIPAA (not to mention requirements of non-preemption state and other federal laws). Assumption of information blocking risks generating many complaints that HIPAA-covered entities are engaging in information blocking, when in fact they are merely trying to comply with their legal obligations to use and disclose information as only permitted by the rules.

A proposal for information exchange and information blocking cannot hold covered entities responsible for HIPAA compliance, but provide no mechanism to ensure that any request for disclosure provides sufficient information to help the covered entity know whether they are permitted to make the disclosure under the HIPAA rules. An acceptable and workable proposal must discuss in detail the obligations of those who make a request. Just to identify a few examples: How would requestors communicate the purpose of their request, such as being a fellow participant in an accountable care organization, so that a covered-entity respondent can judge whether responding to the request meets HIPAA requirements? What are the guardrails for reasonable requests that would ensure that the request is only to share minimum necessary information that a covered entity is permitted to disclose? Alternatively, a workable proposal would require every requestor to abide by the requirements of HIPAA, whether the requestor is a HIPAA-covered entity or not.

We look forward to working with you as the work the RFI has initiated advances. If you have any questions concerning our comments, please feel free to contact me or Lawrence Hughes, AHA assistant general counsel, at 202-626-2346 or lhughes@aha.org.

Sincerely,

/s/

Melinda Reid Hatton
General Counsel