America's Health Insurance Plans
601 Pennsylvania Avenue, NW
South Building, Suite Five Hundred
Washington, DC 20004

February 12, 2019

Submitted Via the Federal eRulemaking Portal www.regulations.gov

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: RFI/RIN 0945– AA00
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue SW
Washington, D.C. 20201

RE: RIN 0945–AA00 / Docket HHS–OCR–0945–AA00

Dear Sir or Madam:

We appreciate the opportunity to offer comments in response to the Request for Information (RFI) on modifying the Health Insurance Portability and Accountability Act (HIPAA) rules to improve coordinated care that was published in the *Federal Register* on December 14, 2018.[1]

America's Health Insurance Plans (AHIP) is the national association whose members provide coverage for health care and related services. Through these offerings, we improve and protect the health and financial security of consumers, families, businesses, communities and the nation. We are committed to market-based solutions and public-private partnerships that improve affordability, value, access and well-being for consumers.

Every American deserves affordable coverage and high-quality care. Health insurance providers are committed to delivering more choices of better quality at lower costs. Our member companies are engaged in a wide variety of activities, programs and product offerings designed to improve access to quality health care.

[1] 83 Fed. Reg. 64302. As stated in the preamble, the RFI seeks to identify regulatory provisions under HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 that may impede the 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 privacy or security of individuals' protected health information (PHI). In addition, the RFI requests information on whether and how the rules could be revised to decrease regulatory burdens, as well as seeking information about any relevant state or other law containing standards that are different from, and perhaps inconsistent with, HIPAA's requirements or potential regulatory changes.

We remain committed to protecting the privacy and security of individual's health care information and are pleased to share our experiences about the best ways the agency can move forward. By working together, we can promote value-based care and improve care coordination to improve the health and financial stability of everyone. **Our experience has demonstrated that overall the HIPAA privacy and security provisions are working well and the requirements have been proven as effective for protecting the privacy of health data. HIPAA has served as the privacy foundation for individuals and covered entities, including health insurance plans, and we continue to rely on these effective provisions in our business operations and policies.**

The HIPAA Privacy Rule was written when paper-based records were predominantly used. The current policy considerations should take into account the ability to support interoperable and secure health information technology, as well as value-based payment models (e.g., e-measures). There are several areas where we believe OCR should focus available resources to explain the privacy requirements, to inform consumers, and to help entities comply with the requirements. Addressing the following areas to assure privacy protections for individuals while enabling the flow of health data in a timely and secure fashion would improve care coordination and health outcomes:

- Federal and state laws and regulations continue to present challenges for sharing certain categories of health information. Specific challenges exist when substance use disorder, HIV-status, mental and behavioral health or other regulated categories of health information are involved. This is particularly frustrating for individuals and their providers caught in delays or lack of access to critical information. Future work with state regulators and new guidance from OCR should be directed at addressing these situations. A particular focus of this work should continue to address the current opioid crisis and how health information can be used and disclosed to help individuals receive treatment to combat and recover from addictions.

- State laws continue to present challenges for health information access and disclosure. Differences in the laws and regulations governing the age of consent for minors to receive certain health care services, parental rights to access children's health information, and the ability of minors to request suppression of their health information continue to create legal and operational complexity and uncertainty. OCR may want to consider whether a federal regulatory standard should be promulgated to preempt state laws thereby streamlining the privacy protocols for the nation.

- Documentation requirements for individuals who are assisting in an individual's care remain a concern for consumers. State laws governing personal representatives, "representative payees," and others who attempt to assist with another's health care have resulted in perceived barriers for consumers and differences in interpretations,

particularly when an individual lacks the time or the resources to obtain official paperwork recognizing these designations. OCR should focus additional guidance and regulations to alleviate the burden on individuals and entities who are acting in good faith when trying to assist in these situations (e.g., a safe harbor from enforcement activities).

- While HIPAA has served as a foundation for privacy and security for covered entities, many entities remain outside HIPAA's scope. In today's electronic environment, many individuals are sharing their health information with software applications, Internet sites, and devices which may store or transmit health data. Medical procedures can be viewed online, on television, or "streamed" via the Internet while being performed. And companies offer genetic or medical tests with the promise of insights into an individual's health profile. OCR should consider more education and outreach to inform consumers about the risks of sharing their health data in scenarios, with a focus on the risks of sharing data without HIPAA's privacy protections in place. In addition, OCR should work with lawmakers and stakeholders to broaden the scope of the HIPAA privacy regulations to non-HIPAA covered entities.

- Recent passage of the European Union's new privacy framework, known as the General Data Protection Regulation (GDPR), has prompted questions about the interaction between U.S. and new international privacy requirements. Affected entities will continue to monitor developments and implementation activities. OCR may want to engage experts and stakeholders in public forums to help health care entities and the consumers they serve better understand the intersection between privacy frameworks and when or how they apply to U.S. consumers and business entities.

We have organized our specific comments in response to the RFI as follows:

- **Part I**: **Issues, Discussions and Recommendations**. Our discussion of and recommendations for the primary issues identified in the RFI; and

- **Part II**: **Survey Results.** Graphics summarizing a non-scientific, voluntary survey that we conducted to capture a "snapshot" of experiences to help inform our response to the RFI and future policy work.

We appreciate the time given to individuals and entities for responding to the RFI. However, many of the issues presented by the RFI require more than 60 days in order to properly evaluate the issues presented and the potential policy implications. Therefore, we encourage OCR to convene public hearings and to seek the input from advisory bodies such as the National Committee on Vital and Health Statistics (NCVHS) before proceeding with future rulemaking on the topics covered by the RFI. Where we recommend that the agency issue guidance, we stand

ready to work with OCR and other public and private stakeholders to vet and offer comments in response before such guidance would become final and binding on affected entities.

We appreciate the opportunity to comment on these important topics. Please contact me at mzluke@ahip.org if you have any questions.

Sincerely,

Marilyn Zigmund Luke
Vice President

AHIP Comments in Response to the RFI on Modifying HIPAA Rules to Improve Coordinated Care

Part I: The RFI Issues, Discussion and Recommendations

February 12, 2019

Care Coordination/Case Management and Value-based Health Care

We support OCR's goals of promoting information sharing for treatment, care coordination, and value-based care. The HIPAA Privacy Rule currently allows for uses and disclosures of health information in the definition of "health care operations" for "activities relating to improving health or reducing health care costs, case management and care coordination."[2] Health insurance plans frequently provide outreach to health care providers and individuals to help promote better care and coordinate access to medically-necessary services. **Overall, care coordination efforts are occurring, and we do not believe that changes to the HIPAA regulatory provisions are required at this time to meet the needs of individuals and their treating health care providers.**

We believe value-based care can help transform the U.S. healthcare system as consumers receive services based on proven measures and health care providers deliver services in ways that reduce administrative burdens and help keep care focused on patient safety and outcomes. Such innovative programs can help to address chronic illnesses, support functional impairments, and promote effective care coordination.

Value-based care continues to evolve. In past years, value-based care arrangements were viewed more as a model or demonstration project whereas current efforts are focused on collaboration with targeted, effective solutions to improve outcomes and drive down health care costs. Currently, multiple quality measures are being used to evaluate healthcare performance, which may be different across payers or settings.

Health insurance plans and health care providers are collaborating on targeted, effective solutions to move us toward accomplishing the Triple Aim®: (1) the individual experience of care; (2) improving the health of populations; and (3) reducing the per capita costs of care for populations. In fact, Medicare Advantage plans are leading the way with nearly 50 percent of their payments flowing through contracts with providers of this nature in 2017.[3] However, these arrangements vary broadly in their scope and impact on consumers (e.g., a percentage of

[2] 45 C.F.R. §164.501.
[3] Healthcare Payment Learning and Action Network, "APM Measurement: Progress of Alternative Payment Models," available at http://hcp-lan.org/workproducts/apm-methodology-2018.pdf.

payment for a particular health care service based on outcomes, models where providers assume risk for the full cost of care).

AHIP, in partnership with the Centers for Medicare & Medicaid Services (CMS) and the National Quality Forum (NQF), leads the Core Quality Measures Collaborative (CQMC) to improve health care quality for every American.[4] Through this collaborative effort, we hope to align quality measures across public and private payers to improve care, reduce provider burden, and share consistent performance information with consumers and payers. The NQF will provide expertise to the CQMC on updating existing core measure sets and expanding into new clinical areas. The NQF will also work collaboratively with CQMC members to develop strategies for facilitating implementation across care settings and promote measure alignment. We would encourage OCR to help improve response time to inquiries around data sharing under the Privacy Rule in these situations.

Defining what constitutes "value-based care" may be helpful as OCR and other agencies evaluate these arrangements to help patients better understand and evaluate their own healthcare while reducing the burden and redundancy for clinicians and healthcare organizations. Any definition should be flexible to allow for future changes in the industry, in the systems, and arrangements that may develop.

Recommendation: Because there is diversity in these types of measures and payment arrangements, future discussions should "level-set" the meaning of "value-based care," while allowing for flexibility to accommodate future developments. OCR may want to begin with a "working definition" and we propose the following definition for consideration:

> **"A program that aligns incentives and promotes a patient-centered approach where treatments are tailored to the individual to ensure it's the best fit for them."**

[4] Originally founded in 2015, the CQMC is a broad-based coalition of health care leaders, including CMS, health insurance providers, primary care and specialty societies, and consumer and employer groups. These leaders have worked together to develop recommended core measure sets to measure the quality of American health care. This collaborative effort is committed to: (1) promoting quality measure alignment across the public and private health care sectors; (2) reducing the reporting burden that measurement causes for providers; (3) improving care quality and health outcomes; and (4) offering consumers actionable information about provider performance to help them make decisions about where to receive their care. More information is available at: https://www.ahip.org/ahip-cms-collaborative-announces-core-sets-of-quality-measures/. Additional resources from AHIP can be found at the following links: https://www.ahip.org/examples-of-our-commitment-to-value-based-care/; https://www.ahip.org/wp-content/uploads/2017/07/The-Key-to-Accelerating-Success-with-Value-Based-Care_An-NTT-DATA-Whitepaper.pdf; and https://www.ahip.org/issues/delivery-payment-system-reform/.

Access Rights

Under the HIPAA Privacy Rule, an individual has the right to access and obtain a copy of his or her PHI. A covered entity must provide access within 30 days after receipt of the request, with the possibility of one 30-day extension. Third parties can obtain access to PHI from an entity when authorized in writing by an individual.

We believe that individuals have been able to access their health information and that no major regulatory changes or clarifications are required at this time. In fact, electronic developments such as online portals that provide access to educational materials, phone-based applications, summaries of health care services, claims payments, notices of privacy practices, upcoming appointments, test results, and other resources have helped consumers obtain information virtually at any time through private, secure Internet-based systems. In our experience, the majority of consumers obtain needed information through these channels rather than submitting a written request for records. Most requests received in writing for access to PHI from individuals or third parties acting on their behalf (e.g., attorneys involved in litigation, domestic matters such as divorce and custody disputes) are for litigation or other legal matters unrelated to direct treatment or care coordination. These requests are being fulfilled timely and meet the consumer's expectations.

We note that as the agency evaluates a need for potential regulatory changes that it is vitally important to not conflate the need of individuals to access their health information with business-to-business data exchanges that occur as part of routine business operations. For example, health information shared between HIPAA covered entities can occur expeditiously and should not be subject to 30-day rules or other regulatory processes. If promulgated, such requirements may have the unintended consequences of slowing data exchanges (e.g., health care provider to health insurance provider; exchanges for health oversight or governmental health benefits programs). Likewise, covered entities already have processes for information requests from individuals or their treating providers that may require a sense of urgency (e.g., coverage of urgent care services). Existing federal regulations[5] and some state requirements can govern the timeframes within which these data exchanges occur. Data transfers for other business functions (e.g., that support payment/contracted amounts) are for different purposes and should remain outside the scope of the 30-day access rules.

We recognize that the CMS is expected to issue regulations (being referred to as the "Blue Button 2.0" proposed rule), to promote the sharing of claims and other health related information with third party vendors as requested by Medicare beneficiaries. However, we are concerned that

[5] The U.S. Department of Labor (DOL) has requirements for "urgent" claims and the appeals processes, 29 C.F.R. § 2560.503-1. *See also,* DOL resources available on the Internet at: https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/resource-center/faqs/benefit-claims-procedure-regulation.

PHI may be shared with vendors who have not been verified for legitimacy and that consumers' PHI and other confidential information may be at risk.

OCR should also work with CMS for the "Blue Button" regulations to clarify individuals' requests to receive their health information or to share it with their health care providers. Different processes for third-party vendor applications, which may or may not be automated, will likely be governed by the "Blue Button" rule. It will be important to distinguish such processes from the individual access rights. In addition, health insurance providers will likely need to establish criteria and processes to vet and identify with which third party vendors they will share individuals' PHI. We plan to submit similar comments to CMS once the regulatory proposals are issued.

Recommendation: We continue to support the individual rights of access and inspection for obtaining their health information. Business-to-business data exchanges, however, do not require regulation as such exchanges currently occur as part of routine business operations.

In 2010, OCR issued an RFI and then a Notice of Proposed Rulemaking. We submitted detailed comments at that time. We were pleased that the 2019 RFI states OCR's opinion that the 2010 proposed access report requirement would create undue burden for covered entities without providing meaningful information to individuals. Thus, OCR intends to withdraw the NPRM.

Recommendation: We support OCR's withdrawal of the Notice of Proposed Rulemaking for access reports.

Social Services Beyond Healthcare

Some individuals, such as those experiencing homelessness or suffering from chronic conditions, including serious mental illness, may receive care from a variety of sources including HIPAA covered entities, social service agencies, and community-based support programs. In addition, some jurisdictions have multi-disciplinary teams that assist in coordinating the full spectrum of care for individuals who need such assistance. Individuals who participate in care management programs may receive referrals or access to social service programs.

Often eligible individuals or those who are in crisis can benefit from information being shared between HIPAA covered and non-covered entities. Before doing so, however, HIPAA covered entities will seek an individual's written authorization before making a disclosure of health information to a non-HIPAA entity, even in situations where well-intentioned employees may be trying to facilitate care or help for an individual (e.g., someone who is homeless, seeking treatment for a substance use disorder, living in a shelter without a parent or guardian, children in foster care situations). Otherwise, a violation and significant penalties could result, particularly

since there is no existing safe-harbor for those acting in good faith who are trying to help an individual obtain housing, health care or other necessary services. Also, clarification from OCR on what constitutes a "social service agency" may be helpful in these situations.

Social services agencies and community-based support programs frequently utilize their resources to benefit the individuals and communities they serve. They often lack the resources to invest in electronic systems, operational policies and procedures, or legal fees to understand, sign, and comply with business associate agreements. An additional consideration would be that if such an entity were given access to an individual's PHI, there may be inadequate measures to further protect the health information from subsequent improper uses or disclosures. Whenever possible, OCR should try to reinforce the disclosure of de-identified data, if those elements could be of use to social service agencies and community-based support programs to help meet the needs of the individuals and communities they serve. In addition, OCR should provide clarity addressing how a social service agency or community-based support program can assist individuals or communities without individuals' names or demographic information.

Certain health benefits programs that are specifically designed to benefit eligible individuals (e.g., Medicare fee-for-service, Medicare Advantage, Medicaid, Children's Health Insurance Programs, state-based prescription assistance) or specific populations (elderly, disabled, indigent, person displaced due to a personal crisis) may benefit from future regulations or guidance that would enable disclosures of and protocols for legitimate disclosures of an individual's PHI to social services and community-based support programs. In addition, public health oversight agencies may consider how or if provisions could be designed to promote information sharing for legitimate social services, based on well-defined and specific situations.

OCR may consider exploring how sharing health information can help affected populations overcome societal affects that can influence health care access and outcomes. Addressing social determinants of health can improve health and well-being and sharing information with community agencies is an important part of addressing these needs. OCR should also discuss the potential consequences of sharing information with these types of agencies (e.g., housing discrimination, custody/foster care situations).

Recommendation: OCR, working in conjunction with federal and state agencies and consumer groups, should contemplate "pilot tests," demonstration projects, or situational use cases to test proposals and protocols for sharing information between HIPAA and specially-designated social services and community-based programs that support individuals in need. This work can help define what constitutes a "social service agency" and can serve as a checklist of steps to take for information sharing procedures between HIPAA covered entities and social service agencies. Such test cases can help inform permitted sharing of PHI without an individual's written authorization, provide incentives for these programs to purchase and use compliant systems, and help inform similar

considerations for these data sharing situations. These experiences can be part of or help build on existing government programs oversight.

Accounting of Disclosures

The Privacy Rule requires covered entities to provide an individual, upon request, with an accounting of certain disclosures of PHI that were made by the covered entity or its business associate during the six years before the request. While the Privacy Rule currently excludes certain disclosures from the accounting requirement, including disclosures made for treatment, payment, and healthcare operations, section 13405(c) of the HITECH Act directs the U.S. Department of Health and Human Services to modify the Privacy Rule to require that an accounting of disclosures include disclosures made for TPO purposes through an electronic health record (EHR) during the three years before the request.

Not all covered entities use EHRs, as that term was defined in the HITECH Act. That definition should be an integral part of OCR's future analysis because the scope of entities covered by the HITECH provision was and continues to be limited to those situations where an EHR is in use.

As discussed above, OCR intends to withdraw the 2010 NPRM and now requests public input to help implement the HITECH Act requirement and ensure that 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 or otherwise, without erecting obstacles or disincentives to the adoption and use of interoperable EHRs, which is necessary for efficient care coordination, case management, and value-based healthcare.

As highlighted in Part II of our response, we share anecdotal information from a recent survey of health insurance providers. As our results indicate, there were extremely few requests for an accounting of disclosures made by individuals in 2018. We continue to support our prior comments and policy positions that we shared with the agency in 2010. The costs of implementing the accounting of disclosures requirement at this time would outweigh the benefits to consumers. We believe that current and better technologies and processes are in place to help consumers get the information they need. And the current Administration would likely support abdicating regulations for private entities that would result in significant costs without a substantial benefit to consumers.[6]

Recommendation: We support OCR's withdrawal of the 2010 NPRM, including the accounting of disclosures proposals. We recommend that OCR seek ways to work with

[6] *See,* Goals outlined by the Secretary of the Department of Health and Human Services include burden reduction where no commensurate benefit to beneficiaries is available. More information is available at the following link: https://www.hhs.gov/sites/default/files/Reforming-Americas-Healthcare-System-Through-Choice-and-Competition.pdf.

Congress, the Administration, and stakeholders to change the HITECH Act requirement so that the Department need not promulgate unnecessary and burdensome regulations. After presenting the state of the electronic capacities that exist within the healthcare system, compliance with the HITECH's provision should be deemed unfeasible for promulgation at this time.

Notices of Privacy Practices

The Privacy Rule requires covered providers and health insurance 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. Covered entities are required to provide their NPPs to individuals, consistent with the specific requirements of the Privacy Rule, including prominent display on their websites. In addition, a covered health care provider that has a direct treatment relationship with the individual must clearly and prominently post the NPP in physical service delivery locations. Providers must also provide the NPP to individuals by the date of first service delivery, and to any individual upon request.

Health insurance providers are accustomed to providing individuals with NPPs. We have long-supported OCR's models to aid compliance and consistency with informing consumers of the NPPs.

Some of our members offer health services through integrated delivery systems. The Privacy Rule requires covered providers that have a direct treatment relationship with an individual to make a good faith effort to obtain a written acknowledgement of receipt of the provider's NPP. If providers are unable to obtain the written acknowledgement, they must document their good faith efforts and the reason for not obtaining an individual's acknowledgment, and the provider must maintain the documentation or proof to support compliance with the requirements for six years.

We would be open to evaluating future policy proposals that would establish a safe harbor for entities that use OCR's Model NPP in full or as part of its own NPP, as well as proposals that would eliminate or modify the obligation for health care providers to make a good faith effort to obtain an acknowledgment of receiving the NPP at the individual's first visit. For example, the HIPAA NPP requirements can be better aligned with federal and state requirements for providing notices electronically, and upon an individual's request. In addition, today's electronic environments and technologies allow individuals to access information, and NPPs are available on website and other electronic modalities to describe data uses and disclosures.

Recommendation: We support ways that care providers with a direct treatment relationship with an individual can reduce administrative burdens and devote available

resources toward direct patient care. Likewise, we are open to evaluating alternate ways for making NPPs available to consumers in more efficient and less-costly ways.

Disclosures for Treatment and Related Purposes

Disclosure of health information for treatment purposes are some of the primary functions for health entities. The HIPAA Privacy Rule incorporated the concept of "minimum necessary" into many disclosures but excluded those made for treatment from this provision. We continue to support treatment disclosures unencumbered by "minimum necessary" review and evaluations.

We also believe that disclosures of PHI to covered entities for care coordination should be exempt from the "minimum necessary" requirement. This would include population-based case management and care coordination activities, claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development as excepted from the minimum necessary requirement.

One issue that we have identified concerns health care providers in certain rural areas making requests of health insurance providers for "data dumps" (i.e., complete disclosures of an individual's health records) of all individuals covered by their products. These providers classify the requests as "treatment," but in practice, it was discovered that the health care providers made voluminous requests in an effort to prepare for an emergency situation. In other words, if a geographical area had a failed Health Information Exchange (HIE) or had no existing electronic functionality for sharing records, some health providers were attempting to compile complete records on individuals in the event any individual presents for care in an emergency situation (e.g., at a hospital). We believe these situations are outside the scope of the HIPAA treatment disclosures, and we encourage OCR to provide guidance and education to alleviate the burdens and risks such requests present for individuals whose information is covered in these requests.

Another area of concern has to do with required reporting for health oversight functions or for governmental health benefits programs. Processes such as HEDIS reporting, audits (e.g., Risk Adjustment Validation Audits [RAD-V]), and similarly-mandated processes require health care providers to send or share information with health insurance plans and other entities. In some cases, there has been a reluctance to disclose such information. Long delays have also been anecdotally reported. These factors may be attributed to a lack of understanding of the uses and disclosures allowed by the HIPAA Privacy Rule. OCR should consider additional guidance to help address these scenarios and/or add these specific processes to the regulations (e.g., under the definition of "payment" in 45 C.F.R. §164.501).

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. While HIPAA has served as a foundation for privacy and security for covered entities, many entities that use and disclose individuals' health information remain outside HIPAA's scope.

In today's electronic environment, many individuals are also sharing their health information with software applications, Internet sites, and devices which may store or transmit health data. Medical procedures can be viewed online, on television, or "streamed" via the Internet while being performed. And companies offer genetic or medical tests with the promise of insights into an individual's health profile.

Recommendation: OCR should consider more education and outreach to inform consumers about the risks of sharing their health data without the HIPAA privacy protections being in place.

If covered entities or non-covered health care providers report difficulties obtaining needed PHI for coordination of care and treatment, then additional guidance and examples of permitted disclosures from OCR may be helpful.

OCR should continue to work with lawmakers and industry stakeholders to expand the scope of HIPAA's privacy regulations to non-HIPAA covered entities.

Coordination with ONC's Priorities

OCR should work collaboratively with other federal agencies to ensure the HIPAA privacy and security rules are understood and implemented. For example, yesterday the Office of the National Coordinator for Health Information Technology (ONC) issued regulations to prohibit "information blocking" (as that term is defined by the 21st Century Cures Act). ONC has also undertaken efforts at promoting the "Blue Button 2.0" initiative, which would promote interoperability and advance the digital exchanges of information.

At present, approximately half of states have an All-Payer Claims Database (APCD) that compiles individuals' health information based on electronic enrollment and/or claims data. Individual written authorization is not required as part of these processes and HIPAA covered entities are required to submit data, including PHI. Many consumers remain unaware that their health data is being used for these purposes or maintained in the APCDs. The ONC's "Blue Button" initiative may take a different approach that may change processes for APCDs, particularly if an individual must consent to or authorize disclosures related to these existing electronic processes.

We also note that ONC is exploring "opt-out" and "opt-in" processes for having health information included as part of an overall strategy for HIEs. We believe that ONC should be

working with OCR to accomplish the goals of improving care coordination and promoting value-based health care. We will continue to monitor and be engaged in the promulgation of future ONC and OCR regulations that cover these policy objectives.

We also anticipate that as ONC moves toward a system that is electronically-based, scenarios may emerge in which electronic inquiries are made by non-legitimate actors or non-HIPAA entities attempting to obtain individual's health or other information. Future federal work should try to anticipate these privacy and security risks and provide clarification for entities that may be facing new interfaces and inquires via digital exchanges.

Recommendation: OCR should engage with ONC to further evaluate policy developments in this area and to assess the downstream implications to HIPAA covered entities and existing data reporting processes. OCR should initiate consumer education programs related to APCDs. OCR should also ensure that its efforts align with ONC policy and initiatives.

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

The Privacy Rule allows covered entities to disclose PHI to caregivers in certain circumstances, including certain emergency circumstances. Given the opioid crisis and efforts to address serious mental illnesses, anecdotal evidence suggests that some covered entities are reluctant to inform and involve the loved ones of individuals facing such health crises for fear of violating HIPAA or applicable state laws governing disclosure of sensitive diagnoses information.

The preamble explains that OCR is considering a separate rulemaking that would seek to encourage covered entities to share PHI with family members, caregivers, and others in a position to avert threats of harm to health and safety, when necessary to promote the health and recovery of those struggling with substance use disorder, including opioid use disorder, and/or serious mental illness (SMI). OCR would like to consider amendments to the Privacy Rule that would allow OCR to address the opioid crisis as well as facilitate parental involvement in the treatment of their children.

We would support future guidance or rulemaking to help individuals who are assisting in another's care. As noted above, state laws governing personal representatives, "representative payees," and others who attempt to assist with another's health care have resulted in perceived barriers for consumers and differences in interpretations, particularly when an individual lacks the time, resources, or mental capacity to obtain official paperwork recognizing these designations. This is further complicated by state laws that restrict disclosure of sensitive information, such as HIV/AIDs, mental health and substance use disorder information even to those who may be involved in assisting in another's care.

There is also a need to coordinate with SAMHSA to create a viable way for entities to exchange information about opioid use. Access to high-quality, coordinated care can be limited by the federal Part 2 substance use disorder regulations.

Recommendations: OCR should focus additional guidance to alleviate the burden on individuals and entities who are acting in good faith when trying to assist in these situations. We support establishing new policies for HIPAA covered entities to better understand how to share PHI with family members, caregivers, and others who are assisting in their care. Likewise, we are open to evaluating future proposals that would promote the health and recovery of individuals with substance use disorders or serious mental and behavioral health illnesses, based on the current needs for sharing information and consumers' preferences for addressing health data in these situations.

Clearinghouses

As defined in the HIPAA statute, a health care clearinghouse is a covered entity defined as "a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements."[7] Clearinghouses can receive health information in their role and would be required to comply with the statutory and regulatory requirements. Historically, trading partner agreements were put in place between health care clearinghouses and other HIPAA covered entities (e.g., health insurance plans, health care providers that conduct electronic transactions).

The RFI presents a different perspective relating to the legal status and role of clearinghouses. The RFI states that clearinghouses "typically receive PHI in their role as business associates of other covered entities and may provide an individual access to that PHI only insofar as required or permitted by their business associate agreement."[8] As a business associate, however, a clearinghouse should only be releasing information as directed by a covered entity and allowed by the written agreement. OCR should issue guidance clarifying those situations in which clearinghouses are acting as business associates as opposed to HIPAA covered entities.

As discussed in the RFI, clearinghouses may maintain PHI from a variety of health care providers.[9] The RFI solicited comments about whether clearinghouses would be a viable source of information for consumers seeking to obtain a complete record of their health information without having to separately request PHI from each health care provider.

[7] 42 U.S. Code §1320d. *See also,* 42 U.S. Code § 1320d–1.
[8] 83 Fed. Reg. 64304.
[9] *Id.*

Consumers are not familiar with health care clearinghouses and the functions they perform. Most consumers would not likely know which clearinghouse their health care provider and/or health insurance plan uses for electronic transactions. Additionally, the data streams that flow between these HIPAA covered entities consist primarily of the data mandated by HIPAA's transactions and code sets. This data would likely exceed the scope of what a consumer needs and would not be the best source of data for someone seeking their own health care record. In most cases, a single clearinghouse would not have a longitudinal history of an individual's health records.

Recommendation: Health care clearinghouses would not be the best data source for consumers who need to obtain their own health information.

Substance Use Disorder Information (42 C.F.R. Part 2)

Federal and state laws and regulations continue to present challenges for sharing certain categories of health information. Specific challenges exist when substance use disorder information is involved.

AHIP, in conjunction with the Substance Abuse and Mental Health Service Administration (SAMHSA) and other stakeholders, have been working for some time on addressing the legal and operational challenges that the federal confidentiality regulations governing substance use disorders (commonly referred to as "42 C.F.R. Part 2" or the "Part 2 regulations") that exist within the health industry. We continue to advocate for alignment of the Part 2 regulations with the HIPAA Privacy Rule, and we recognize that a statutory change may need to be effectuated before SAMHSA can make progress in response. Unlike HIPAA, we believe the federal confidentiality regulations governing substance use disorders can impede care coordination and value-based care. There is also a need to address situations where an individual is unable to authorize or consent to information disclosures because the individual lacks the legal ability (e.g., is incapacitated, is impaired by a substance).

Recommendation: OCR should continue to support alignment of the HIPAA Privacy Rule with the 42 C.F.R. Part 2 requirements. OCR should delay future rulemaking on this topic until Congressional activity is made final. OCR should also seek opportunities to coordinate with SAMHSA.

HIPAA Coordination with Other Laws

Recent passage of the European Union's new privacy framework, the GDPR, has prompted questions about the interaction between U.S. and new international privacy requirements. There have also been emerging proposed state specific privacy laws in California, Oregon, Utah, Virginia, Washington and Wyoming governing portions of what is addressed under GDPR.

When the HIPAA statute was enacted and subsequent privacy regulations were issued, it was well-established that State laws and regulations would remain in place as long as they were not contrary to HIPAA and they provided greater privacy protections for individuals. HIPAA was intended as a "federal floor" and the States could build on these privacy requirements.

State laws have presented and continue to present challenges for health information access and disclosure. While HIPAA does not contain a private right of action for individuals to sue, some states differ, and enforcement of alleged privacy violations can occur at the federal and state levels. This has created legal complexity and difficulty for entities trying to understand the jurisdiction of various regulators and the uses and disclosures of information, particularly when individuals' health information is encompassed by or is the subject of inquiries and legal actions. States laws with sweeping privacy requirements can be challenging to reconcile with the HIPAA rules.[10] Differences in the laws and regulations governing parental rights, minors, spousal restrictions on accessing health information and the handling of reduced-capacity or incapacitated individuals in the health care system has resulted in a variety of interpretations. The age of consent for minors to receive certain health care services varies State to State, parental rights to access children's health information can be restricted, and the ability of minors to request suppression of their health information continue to create legal complexity and uncertainty.[11] These are priority matters that OCR should address through guidance and future public outreach.

Specific challenges also exist when substance use disorder, HIV-status, mental and behavioral health, genetic, or other regulated categories of health information are involved. In addition to the federal Part 2 rules discussed above, some States have different regulations for special categories of health services and related or restricted information sharing. OCR should help facilitate a better understanding of these situations and how entities can comply in these scenarios.

---

[10] California Consumer Privacy Act of 2018, Cal. Civil Code §§ 1798.100 - 1798.199. While at least nine other state courts (Delaware, Kentucky, Maine, Minnesota, Montana, North Carolina, Tennessee, Utah and West Virginia) have looked to HIPAA to evaluate the relevant standard of care, the Connecticut Supreme Court appears to be the first to actually declare that HIPAA establishes a standard of care. *See*, David Harlow, HIPAA: Liability to private parties for violations, MedCityNews.com (November 16, 2014): https://medcitynews.com/2014/11/hipaa-liability-private-parties-violations/.

[11] In Pennsylvania, the age of consent is 14. Alabama has a similar age for minors to obtain health services, but allows children at age 12 to consent to certain types of care (e.g., gynecological services). *See*, Code of Alabama, Section 22-11A-19 (minor 12 years or older may consent to medical treatment for sexually transmitted disease); Code of Alabama, Section 22-8-6 (consent of any minor as to pregnancy, venereal disease, drug dependency, alcohol toxicity and reportable disease); Code of Alabama, Section 22-8-4 (any minor who is 14 years of age or older, or has graduated from high school, or is married or having been married is divorced, or is pregnant, may give effective consent to any legally authorized medical, dental, health or mental health services). Note: Minors can consent to limited services as listed above prior to age 14, but upon age 14, the minor can consent to all health care without parental involvement/consent. *See also,* Minor Consent to Medical Treatment Laws, National District Attorneys Association https://ndaa.org/wp-content/uploads/Minor-Consent-to-Medical-Treatment-2.pdf.

Another example is the relation of the HITECH Act data breach reporting rules and new federal interpretations and applications of these rules. Data breach and reporting processes have been subject to a variety of interpretations that have changed the definitions for and handling of "security incidents," cybersecurity campaigns, and data breaches. Federal health benefits programs such as Medicare Advantage and the Federal Employees Health Benefits Program (FEHBP) have implemented their own contractual expectations and guidance for HIPAA covered entities that work with these health benefits programs. Compliance challenges have resulted for entities that must adhere to HIPAA's and the HITECH Act's jurisdiction that have been changed by the variety of federal agencies' views, interpretations, and ongoing implementation of these requirements.

Also, the Telephone Consumer Protection Act (TCPA) and corresponding regulations have been challenging for care management. The regulations give the Commission the authority to determine exceptions for informational messages that are autodialed or prerecorded messages to cell phones or texts. The Commission has discussed an exception for healthcare providers sending health care related messages but did not encompass all HIPAA entities that conduct care management (e.g., permissible messages such as flu shot reminders and other preventive measures sent by health insurance providers) in the permissible activities.

Recommendation: Future work and new guidance from OCR should be directed at addressing the challenges with State laws and the HIPAA Privacy Rule. A particular focus of this work should address the current opioid crisis and how health information can be used and disclosed to help individuals combat and recover from addictions.

OCR should consider compiling an inventory of State laws and regulations and guidance of the interaction with federal HIPAA Rule and the HITECH Act's statutory and regulatory privacy requirements.

Dialog in public forums may help health care entities and the consumers they serve better understand the intersection between privacy frameworks and when or how they apply to U.S. consumers and business entities.

OCR may also want to consider whether a federal regulatory standard should be promulgated to preempt state laws thereby streamlining the privacy protocols for the nation, and should work with lawmakers to achieve such uniformity.

AHIP Comments in Response to the RFI on Modifying HIPAA Rules to Improve Coordinated Care

Part II: Survey Results

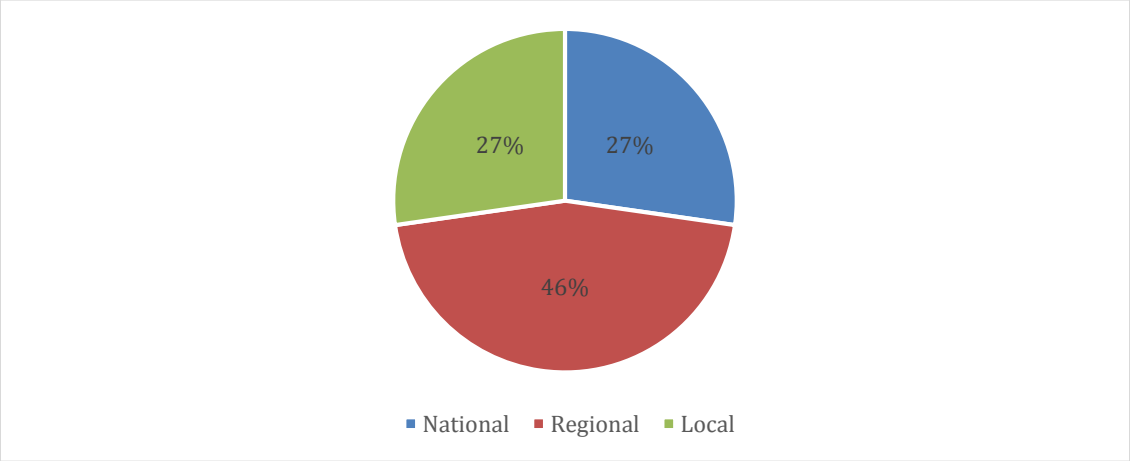
February 12, 2019

In preparing our response to the RFI, we conducted a voluntary, non-scientific survey of our members to provide a "snapshot" of data to supplement the anecdotal information we received and to assess the current status of experiences and opinions. What follows below are graphics summarizing the results received to date.

We offer these data to help inform our recommendations and our future policy discussions. We highlight the "data points" below for those priority areas discussed in the RFI and where we believe the agency should devote resources for refining and clarifying the issues presented to consumers in the current health care environment. The data below were based on 10 organizational respondents.

Data Point #1: The survey respondents characterize their organizations as follows:

- A "local company" (i.e., operating in no more than one state)
- A "regional company" (i.e., operating in more than one state)
- A "national company" (i.e., operating in all 50 states)

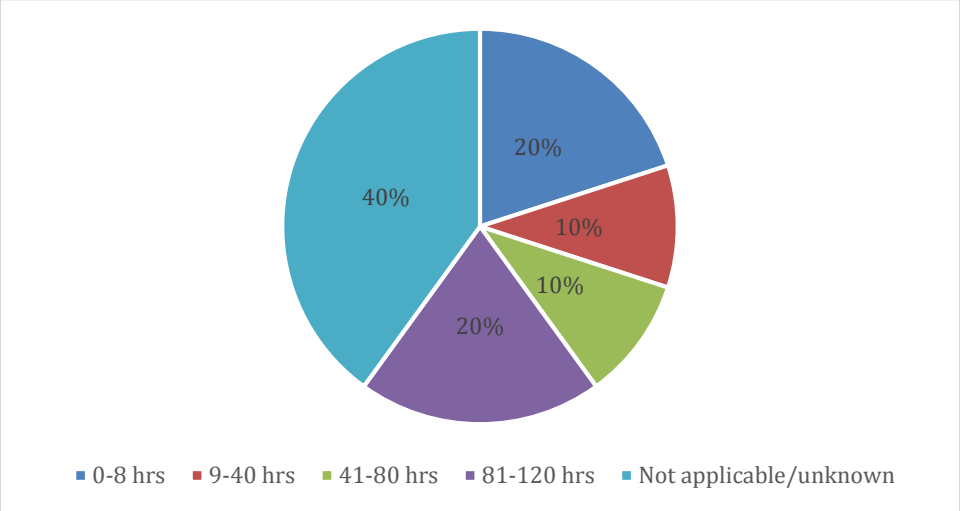


Data Point #2: For the period January 1 – December 31, 2018, the following requests for an accounting of disclosures were received by responding organizations.

Percentage of Accounting of Disclosures Requests Received by an Organization Compared to the Total Population (i.e., Covered Lives)

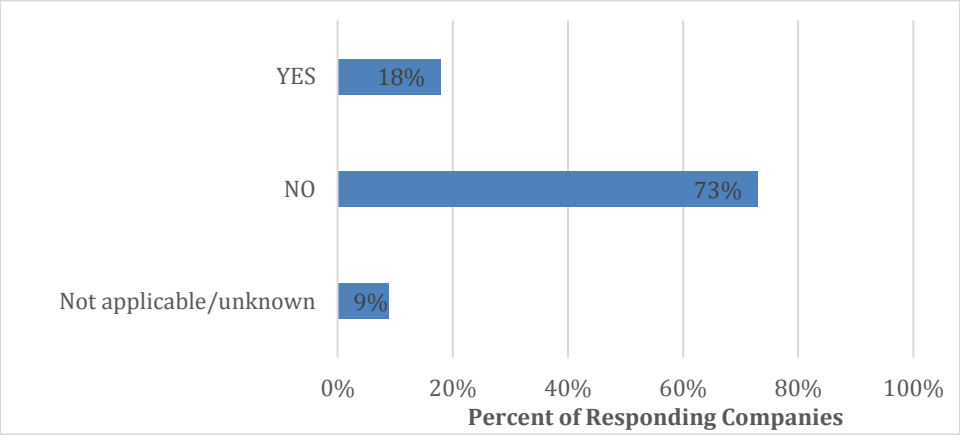
Respondent A	0.000006%
Respondent B	0.000392%
Respondent C	0.003380%
Respondent D	0%
Respondent E	0%
Respondent F	0%
Respondent G	0%
Respondent H	0%
Respondent I	0%
Respondent J	0%

Data Point #3: Please provide an estimate of how much time on average it takes for your organization to produce an individual's request for an accounting of disclosures.

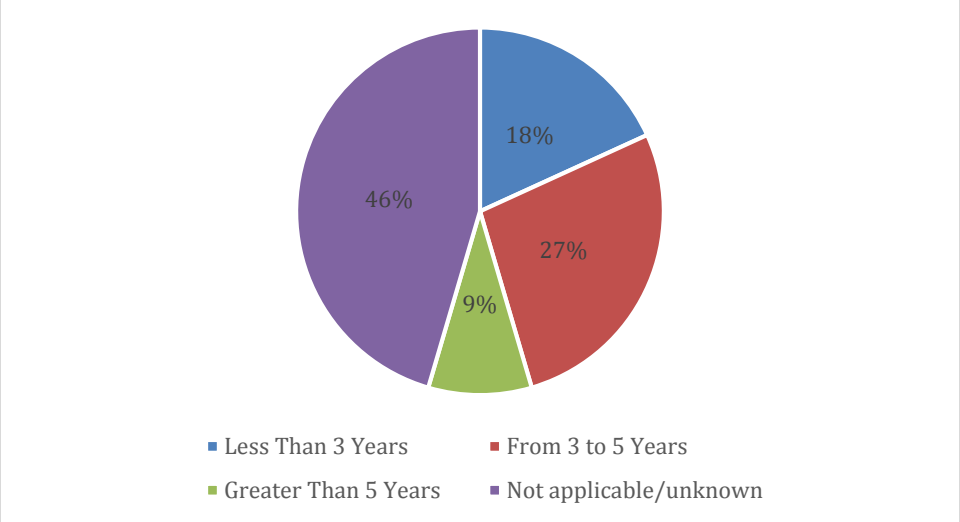


Data Point #4: No respondent reported receiving a specific request from an individual to receive the accounting of disclosures in electronic form.

Data Point #5: Respondents indicated whether their organization allows one or more business associates to directly provide individuals with an accounting of disclosures.



Data Point #6: If regulatory changes to the accounting for disclosures requirement were implemented, the following estimate the "lead time" that would be needed to comply with the requirements.



Data Point #7: The following potential burdens/anecdotal information were identified for covered entities if the accounting for disclosures requirements were expanded to include additional uses and disclosures:

- Significant Information Technology Expenses (e.g., design, testing, production)
- Increased Administrative Costs
- Increased Documentation/Administrative Requirements
- Hiring Additional Staff
- Compiling Members' Written Authorizations
- Minimal Benefit to the Individual Member/Patient
- Unable to Estimate at this Time

Data Point #8: The estimated implementation costs were hypothesized if new regulatory changes are required to modify information technology systems for making changes to the accounting for disclosures processes.