CIVITAS
Networks for Health

September 28, 2023

Bill Cassidy, M.D.
Ranking Member
Senate HELP Committee
428 Senate Dirksen Office Building
Washington, DC 20510

RE: Request for Information from Stakeholders on Improving Americans' Health Data Privacy

Dear Ranking Member Cassidy:

Civitas Networks for Health (Civitas) appreciates the opportunity to provide feedback on the September 7, 2023, request for information (RFI) from stakeholders on improving Americans' health data privacy issued in your capacity as Ranking Member of the Senate Health, Education, Labor, and Pensions (HELP) Committee. Civitas is a national nonprofit collaborative comprised of more than 165 member organizations—health information exchanges (HIEs), regional health improvement collaboratives (RHICs), and providers of services to meet their needs—working to use data frameworks, information infrastructure, and multi-stakeholder, cross-sector approaches to improve health for individuals and communities. We educate, promote, and influence both the private sector and policymakers on matters of interoperability, quality, coordination, and cost-effectiveness within the health system, while also supporting multi-site, grant-funded programs and projects around the country. As health data at the state, regional, and local level increasingly evolves from bi-directional information exchange into a wider array of clinical, analytic and community benefit functions consistent with the health data utility model (HDU), Civitas is proud to be a critical voice for our members and the communities they serve.

While many of the questions and topic areas included in your RFI overlap with Civitas' work and the activities of our members, we want to highlight the following key points which underscore the priorities for public-interest health data infrastructure in any future update to the Health Insurance Portability and Accountability Act (HIPAA) or related federal legislation:

General Privacy Question—is health data only governed by HIPAA, or are there other types of health data not governed by HIPAA?

Health data is the currency of Civitas members. Our HIE member organizations are secure, flexible, and efficient conduits for it in their service areas; our RHIC members work to systemically analyze and refine it as a tool for quality improvement; and both types of organizations collaborate with a broad array of primary and specialty care providers, hospitals, MCOs, public health authorities, and community-based organizations (CBOs) to use data for strengthening the health system as a whole. The breadth of our members' activities, practical experience, and emphasis on multi-stakeholder collaboration means that we take an expansive view of individuals' "health data."

For Civitas, it includes both protected health information (PHI) as currently defined by the HIPAA Privacy Rule and personal information with substantial impact on health outcomes (and health system utilization) that falls outside HIPAA jurisdiction. The second category is primarily information related to patients' social determinants of health (SDOH), which HHS has defined as "economic and social conditions which influence the health of people and communities." These conditions include housing insecurity, food insecurity, transportation needs, and utility insecurity (four needs specifically mentioned in CMS' 2024 physician fee schedule proposal to cover generalized SDOH assessments under Medicare) as well as broad but critical factors like education and health literacy, household income, geographic distance to care, justice system involvement, and environmental exposure.

Bringing this essential but highly fragmented data under a revised HIPAA or similar framework would be extremely difficult, in part because of the sheer amount of information involved (much of which is not really private by its very nature, e.g., means of transportation, housing status) and in part because standardized methods of measuring and coding such data at scale for clinical use are still under development by public health authorities and organizations around the country (including Civitas). Knowledge of HIPAA procedures for the exchange of PHI among many community-based organizations that do not provide clinical services but make use of clinical data is also lacking, which hinders their ability to make use of PHI from providers and integrate those data streams into their operations. Some SDOH data also falls within the boundaries of other privacy laws, including the longstanding Federal Educational Rights and Privacy Act (FERPA) which governs important health and social welfare information collected by schools that is frequently not shared with HIPAA covered entities. Behavioral health and substance abuse information is particularly valuable for effective care coordination to help youth in need and their families access treatment; yet as HIEs and RHICS have made a concerted effort in recent years to enroll those providers and expand services, they have repeatedly run into administrative delays stemming from HIPAA-FERPA confusion from providers and school districts.

As a solution, any statutory updates to HIPAA should make a point to include provisions that directly address the uncertainty, confusion and resulting connectivity breakdown at the intersection of PHI and SDOH data sources. The legislation should explicitly recognize non-provider CBOs and clearly place PHI that they already share under the HIPAA umbrella, while also clarifying the relationship between HIPAA and FERPA coverage of student data. All physical and behavioral health data currently maintained by K-12 schools and institutions of higher education under FERPA "educational records" should be designated as HIPAA PHI to bring it into alignment with how the same information is handled by virtually every other significant actor in the health data pipeline, thereby minimizing confusion and streamlining exchange operations for the benefit of schools, providers, and students.

Health Information Under HIPAA—how should the sharing of health data across state lines be structured to account for different legal frameworks?

Civitas HIE and RHIC members are state and regional organizations governed by stakeholders drawn from (and ultimately accountable to) the same service areas, carrying out public health missions to enhance connectivity, quality, and efficiency "on the ground" under a variety of state-level data collection and consent structures that exist alongside HIPAA. Our HIE members'

infrastructure forms the backbone of emerging health data utilities (HDUs) in a growing number of states, and our RHIC members utilize this infrastructure to deliver and integrate value-added services including provider performance assessment and improvement programs, population health analytics, care coordination, community outreach, and associated training for auxiliary clinical personnel (among other services).

What all of our members have in common is that they have been built from the ground up in their respective state and regional environments, which include the technical and legal structures that shape health systems as well as the wider socio-political characteristics of their communities which ultimately determine health policy choices and outcomes. This proximity to the people they serve is why Civitas members are effective in their work. From a network architecture perspective, they constitute the essential "local roads" that national health data-sharing "highways" (such as TEFCA) will depend on for sustained impact.

Within this context, most Civitas members operating as business associates under HIPAA share substantial amounts of PHI across state lines with covered entities, public health authorities (PHAs), and other business associates (including other HIEs and RHICs) on a daily basis pursuant to covered entity agreements. Cross-state data sharing volume reflects the reality that most patients create medical records with out-of-state providers at some point, and tens of millions of Americans receive out-of-state care on a regular basis. The dynamic is particularly acute for statewide HIE systems in geographically small states (Vermont, Rhode Island) and those HIEs and RHICs whose service areas cover large cross-state metropolitan areas (greater New York, Philadelphia, El Paso, Kansas City), as well as HDUs that are officially recognized in multiple states (Nebraska-Iowa, Arizona-Colorado). This sharing has been made technically possible on a large scale by the sector-wide emphasis on system interoperability over the past decade, including the advent of the HL7 FHIR standard; ONC's USCDI data elements; and the Information Blocking Final Rule that is now in effect as a result of the 21st Century Cures Act. The Information Blocking Final Rule complements the HIPAA Privacy Rule's longstanding covered entity-business associate agreement framework in providing a legal foundation for practical interoperability and health data sharing.

However, as a consequence of recent Supreme Court decisions, increasing emphasis on behavioral health, and growing awareness of consumer data misuse, there is now far less certainty among Civitas members (and many other health system stakeholders) surrounding the long-term legal relationships between the Cures Act's Information Blocking Final Rule "privacy exception" that exists via ONC rulemaking authority; the "permits but does not require" and law enforcement disclosure standards under the HIPAA Privacy Rule; and the growing patchwork of state-level health data laws and other initiatives intended to protect sensitive health data or otherwise assert jurisdiction over personal data (as well as state-federal relations vis-à-vis these laws). In 2023 alone, new personal data privacy laws have entered into force in California, Utah, Virginia, Colorado, and Washington State with varying definitions of "sensitive data" and HIPAA-related exemptions. The new state laws are in some cases more stringent than HIPAA, most notably with respect to how they allocate liability for consent authorization and the responsibilities for parties receiving the sensitive data in question.

Any legislative revision or update to HIPAA would be a valuable opportunity to stabilize the situation by explicitly recognizing each state's power to define "sensitive data" as it sees fit and develop its own statewide consent management standard if it chooses. An updated HIPAA should further write the Information Blocking Rule's privacy exception into federal law with reference to privacy as state-defined "sensitive data." With such a statutory framework in place, federal regulators at ONC would then have the option of working with states to create standardized, filterable code sets for various types of sensitive data to facilitate interoperability across state lines in accordance with each state's data protection regime and the needs of stakeholders.

An updated HIPAA should also directly and explicitly address the emerging discrepancies between federal and state divisions of responsibility for the senders and recipients of PHI and state-defined sensitive data. In the experience of Civitas members, information sharing is most efficient when it is made incumbent upon information senders to ensure that consent authorizations and other applicable authorities to share are in place. HIEs and emerging HDUs are particularly well-suited to this role in interstate exchange, given their statewide service areas, familiarity with state laws, and technical capacity to securely filter large datasets before information is transmitted out of state—lessening the burden that would otherwise fall on each provider and localized EHR system while building trust. Clarifying these roles will be even more important as the nationwide TEFCA framework builds momentum over the next few years.

Sharing of Health Data—should there be an opt-in method of data collection for health data outside of the HIPAA framework versus an opt-out method? Please Explain.

Having members that are deeply embedded in both clinical and non-clinical service provision in (almost) every state has given Civitas meaningful insight into the benefits and drawbacks of different operating procedures, including "opt-in" versus "opt-out" consent frameworks. In this case, the choice is not particularly close: only a few Civitas members are currently required by state law to have some version of a blanket opt-in permission structure for sharing patient health data, because most of our members find that the process creates a bottleneck at the point of entry that hampers their ability to collect information and trends toward information siloing that undermines HIE goals. The most dynamic HIEs are those which transit large volumes of patient data (both secure PHI and de-identified data) representing substantial shares of their service area populations to maximize their value for participating providers, payers, public health authorities, and other stakeholders, while minimizing administrative burdens and inefficiencies. While some HIEs and emerging HDU systems built on affirmative consent have achieved these aims (notably in New York), on balance the opt-out structures with some specific opt-in requirements (such as for substance abuse information) are more efficient in this regard.

The treatment of health data outside HIPAA's current jurisdiction is another area where opt-in versus opt-out distinctions can be drawn. As noted above, much of this data tracks social determinant factors that providers, public health authorities, and the broader health policy community have only started to take seriously in recent years as a result of research showcasing population health disparities and cost savings. Civitas' RHIC members in particular have been leaders in operationalizing SDOH data through provider quality improvement assessments and standards development (including Civitas' own Gravity Project standards that are being piloted in four states), which requires access to large amounts of secure information from multiple public

and private sources over an extended period. Within their service areas, RHICs also provide technical assistance as well as direct community outreach to further care coordination programs and build referral networks that bring together providers and community organizations around specific issues (e.g., maternal mortality). There is a strong argument to be made for bringing nonprofit CBOs and social care organizations that share large amounts of health data under a revised HIPAA umbrella as a function of their expanding partnerships with covered entities and other business associates; however, a national opt-in mandate should not be under consideration. RHICs and other Civitas members' value-added activities would not be possible—or would at least be significantly more limited and time consuming—under HIPAA revisions that placed SDOH data under a national affirmative consent framework.

Artificial Intelligence—to what extent should patients be able to opt-out of datasets used to inform algorithmic development? How could an opt-out mechanism be structured?

Civitas full member organizations are public and nonprofit entities with statewide or regional service areas and yearly operational revenues drawn from varying combinations of user fee structures, Medicaid formula allocations, and state budget mechanisms. Developing artificial intelligence algorithms "in house" is not within our members' current purview or capabilities. However, many of our members do expect to deploy AI functions at scale in the near-to-intermediate future as "plug-in" applications offered by national vendors in a competitive marketplace or integrated into other off-the-shelf software packages, similar to how they currently employ IT solutions for cybersecurity, cloud storage, and other specific needs. In a few cases, Civitas HIE members have begun to explore AI pilot partnerships with vendors organized around disease surveillance, though these discussions are still in their early stages.

Health information exchanges have high expectations for the ability of AI to enhance existing data aggregation, "clean" patient records (sync and de-duplicate records via matching algorithms), and—perhaps most importantly—advance interoperability through the use of natural language processing (NLP) algorithms that synchronously convert unstructured notes on different platforms into common machine-readable formats. At the same time, Civitas' health improvement collaboratives and value-based care organizations expect that AI integration will help them unlock new insights into population health and systemic efficiencies (or inefficiencies) across both health and social service ecosystems by applying predictive analytic models to large multi-source datasets that incorporate disease surveillance, demographics, payer claims, and more. At the top end of this capability, AI analytics could be used to generate "synthetic" data from large volumes of de-identified patient records that clinicians and public health authorities can in turn use to "train" their MLP algorithms for highly specific projects in their service areas.

In order for our members to fully realize the benefits of these capabilities for the people they serve and the health system at large, any federal legislation on health AI applications should take care not to impose specific consent requirements beyond those which already apply (or would apply under future legislation) to covered entities and business associates—i.e., the HIPAA Privacy Rule's operational consent and right to request requirements, as well as its broad allowance for the sharing of PHI by covered entities and business associates with PHAs (via explicit associate agreements) for public health purposes. All of our members work extensively with state and local PHAs on a regular basis to enable data exchange that improves response and resource allocation

(and increasingly, for value-based assessment, training, and care coordination) as a core part of fulfilling their public-service mandates, which makes the current HIPAA PHA framework invaluable.

Civitas does not feel that the use of AI for data management or analytic purposes necessarily raises privacy concerns at this stage which would be new or substantially different from those raised by current or previous generations of software, especially given that AI applications in their mature forms are likely to provide better privacy protections and overall information security. The same machine learning that can spot small statistical movements in vast reams of data and harmonize data sharing formats can also continuously monitor data usage patterns by covered entities and business associates, raise alerts, and maintain de-identified structures that make authorized attribution much more difficult. Given this reality, a new AI-specific consent framework would add more layers of costly and time-consuming administrative bloat for no clear advantage.

Thank you again for the opportunity to comment. Please do not hesitate to reach out to Civitas if we can be a resource as we work together to achieve a community-governed, interoperable health data system to improve public health and health care outcomes.

Sincerely,

Lisa Bari
CEO, Civitas Networks for Health
lbari@civitasforhealth.org