



Submitted through [www.regulations.gov](http://www.regulations.gov)

March 6, 2023

Director Angela Thi Bennett  
National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue NW, Room 4725  
Washington, DC 20230

**RE: Privacy, Equity, and Civil Rights Request for Comment [NTIA– 2023–0001]**

Dear Director Bennett:

The Confidentiality Coalition appreciates the opportunity to provide comments on the National Telecommunications and Information Administration (NTIA) Request for Comment addressing issues at the intersection of privacy, equity, and civil rights.

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, and others, committed to advancing effective health information privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

**1. Framing**

The NTIA asks how regulators should approach the civil rights and equity implications of commercial data collection and processing, and specifically, how discussions of privacy and fairness in automated decision-making approach the concepts of “sensitive” information and “non-sensitive” information, and the different kinds of privacy harms made possible by each. In the case of certain health information, it is important to keep in mind the existing privacy framework established pursuant to the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations, as amended by the Health Information Technology for Economic and Clinical Health

(HITECH) Act. The HIPAA privacy and security regulations (HIPAA Rules) provide robust privacy and security protections for protected health information (PHI) and should remain the primary privacy legal framework governing health data that falls within its ambit.

Since their implementation over 20 years ago, the HIPAA rules have engendered public trust that individually identifiable health information collected by health care providers and health plans and entities acting on their behalf (HIPAA entities) would be used and disclosed only for healthcare functions such as treatment, payment processing, and safety, and not used or disclosed for other purposes without an individual's authorization. HIPAA covered entities are required to provide individuals with a detailed Notice of Privacy Practices that informs individuals of their privacy rights and how these may be exercised, as well as describing the permitted and required uses and disclosures of PHI. The HIPAA Rules also require the implementation of risk-based administrative, technical, and physical safeguards to protect PHI, and the HIPAA Security Rule is designed to be technology-neutral and scalable. This allows organizations the flexibility to implement policies and controls commensurate with the level of risks they have identified and for security controls to evolve as technology and security threats become more sophisticated.

Any future legislation or rulemaking that addresses individually identifiable health information should focus on health information that is not already subject to comprehensive federal privacy and security regulation, should not be inconsistent with or undermine the HIPAA Rules, or disrupt day to day practices for HIPAA entities. The law should align with HIPAA's definitions, including the definition of de-identified information, and should adopt a risk-based approach for the development and implementation of security controls like HIPAA.

## **2. Impact of Data Collection and Processing on Marginalized Groups**

The NTIA asks about the ways the specific circumstances of people with disabilities create particular privacy interests or risks, and how specific data collection practices potentially create or reinforce discriminatory obstacles for marginalized groups seeking public benefits and accommodations. Methods for collecting information for public benefit should be designed with accessibility and privacy in mind from the outset. There should be multiple formats to accommodate those with different needs. A point of contact, trained in appropriate privacy protocols, should be listed for additional support if additional accommodation or accessibility is needed. Forms should also be made available, secure, and easy to use through all common modalities, including computers, tablets, and smart phones.

People with intellectual or developmental disabilities generally have difficulty entering the personal information requested for services, and often need to rely on others to help them, or to do it on their behalf. For example, a family member or legal representative, such as a guardian, may report an individual's wages to the Social Security Administration. Often, it may take several months for a representative to get access to the individual's employer's human resources system in order to support the individual in

completing their regularly required forms for pay. In addition to software and system access issues, access to or ownership of hardware (e.g., phone, tablets, computers) is also a barrier for marginalized people that may impact privacy when completing digital forms.

In order to mitigate or reduce the discriminatory obstacles for marginalized groups seeking access to key opportunities, such as housing or education or employment, we recommend that demographic data be leveraged to improve health equity and outcomes. Demographic data such as race, ethnicity, religion, sexual orientation, gender identity, and disability status should be used to promote individual and public health initiatives, including addressing health disparities. Demographic data should not be used to discriminate against any individual or group of individuals, and civil rights laws should be used to ensure that this is the case. Standard setting organizations should work with public and private entities to determine how best to collect data that will be used to reduce discrimination and improve health equity, while complying with the HIPAA principle of “minimum necessary.” Entities offering digital tools should be required to embed consumer privacy and security protections within those tools, although ultimately a comprehensive national privacy law is the only effective way to ensure consistent protection of health information that is not currently subject to federal privacy regulation such as HIPAA.

The NTIA also asks whether there are any contexts in which commercial data collection and processing occur that warrant particularly rigorous scrutiny for their potential to cause disproportionate harm or enable discrimination and gives the examples of data collected in the context of healthcare, employment, or credit evaluation. We provide the following recommendations to mitigate these concerns:

- **Agencies should consider incorporating broader data equity research and updates.** Algorithms learn from existing data. Historically, certain populations have been underrepresented and misrepresented in data cohorts. Larger conversations regarding data representation and accuracy, while respecting laws and regulations protecting consumer privacy and rights, are necessary to improve model development and performance. We, therefore, recommend policy makers consider data equity and quality considerations as part of comprehensive equity discussions.
- **Develop further understanding of data processing techniques that distinguish between adverse bias and beneficial bias.** In healthcare, artificial intelligence (AI) may utilize race and gender data to help streamline targeted interventions and create more precise recommendations to benefit a population. We recommend continued collaboration across healthcare stakeholders, including ongoing efforts to define and mitigate potential forms of adverse bias, that can be introduced in healthcare applications.
- **Issues of bias should be considered throughout the lifecycle of algorithms.** Adverse bias issues should be considered throughout the development and

implementation of algorithms, and not simply with respect to specific data elements incorporated into the AI model. This is an evolving field, and we support the continued research and development of principles, standards, and guidelines for algorithm documentation, testing, and auditing, especially for algorithms with a high impact on consumers. We recommend consideration of the complete algorithm lifecycle when developing related guidance. We also support ongoing education and incorporation of input from stakeholders implementing certain algorithms, such as clinicians, as well as those impacted by algorithms, such as patients.

- **Leverage and align with ongoing AI initiatives** around best practices, including the congressionally-supported National Institute of Standards and Technology (NIST) work to develop the [AI Risk Management Framework \(AI RMF v1\)](#) and draft guidelines [for identifying and mitigating bias in AI](#).

### **3. Existing Privacy and Civil Rights Laws**

The NTIA asks whether existing laws and regulations sufficiently address the privacy harms experienced by underserved or marginalized groups, and if any of these provides a useful model. We believe HIPAA provides a useful model for the regulation of individually identifiable health information that falls outside HIPAA. Thus, for example, individuals should be given clear, succinct notice concerning collection, use and disclosure of their health data and their privacy rights. Individual authorization processes (including revocation of authorization) should be written in a meaningful and understandable manner and should be easily accessible to individuals and their designated representatives prior to and after information is used or shared.


Regarding the best ways to collect and use information about race, sex, or other protected characteristics to identify and prevent potential bias or discrimination, we recommend leveraging and aligning with ongoing AI initiatives. As noted above, best practices and guidelines for AI risk management are developing and may vary by context and impact. This includes the Congressionally-supported work from NIST on promoting AI trustworthiness and mitigating risks. Additionally, we note that the collection of race, sex or other protected characteristics can support sufficient bias testing of algorithms. A recent AHRQ study on [“Impact of Healthcare Algorithms on Racial and Ethnic Disparities in Health and Healthcare”](#) found that “disparities were reduced when race and ethnicity were incorporated in an intentional effort to tackle known racial and ethnic disparities in resource allocation.”

### **4. Solutions**

The NTIA asks what principles should guide the Administration in addressing disproportionate harms experienced by underserved or marginalized groups due to commercial data collection, processing, and sharing. We believe that health information should be subject to privacy and security protections commensurate with those under the HIPAA Rules, regardless of who holds or accesses the data. Civil rights laws remain the most effective regulatory vehicle to protect against discriminatory practices, including the use of data in a manner that harms underserved or marginalized groups.

The Confidentiality Coalition looks forward to working with NTIA on steps to protect individuals' privacy as the field of algorithmic science grows in scope and practice. Please contact me at [tgrande@hlc.org](mailto:tgrande@hlc.org) or 202-449-3433 with any questions.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large, looped initial "T".

Tina O. Grande  
Chair, Confidentiality Coalition and  
Executive VP, Policy, Healthcare Leadership Council