



October 31, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue NW, Suite CC-5610 (Annex B)
Washington, D.C. 20580

Re: Advance Notice of Proposed Rulemaking on the Prevalence of Commercial Surveillance and Data Security Practices that Harm Consumers (Commercial Surveillance ANPR, R111004)

Dear Chair Khan:

The Confidentiality Coalition appreciates the opportunity to submit comments on the Advance Notice of Proposed Rulemaking (ANPR) on the prevalence of commercial surveillance and data security practices that harm consumers published by the Federal Trade Commission (FTC) in the Federal Register on August 22, 2022.¹

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.

The FTC asks for comments on the extent to which the collection, processing and retention of consumer data, as well as lax data security practices, may harm consumers, and approaches for addressing this. The FTC also asks whether any types of consumer data, such as health or financial data, should be considered or treated differently.

The Confidentiality Coalition believes that it is important to recognize the distinct nature and role of health data, which is used and disclosed by health care providers and health plans to provide access to and delivery of healthcare, and to enable patients to better manage their care. The Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations provide a robust framework of privacy and security protections for individually identifiable health

¹ 87 Fed. Reg, 51273 (August 22, 2022).

data in the hands of HIPAA covered entities and their business associates that has engendered significant public support and trust over the more than 20 years it has been in effect. Care should be taken to keep this framework in place and not disturb the careful regulatory balance the Department of Health and Human Services (HHS) has maintained to facilitate the beneficial exchange of patient health data while ensuring that it is not misused.


However, HIPAA covers only a subset of individually identifiable health information, namely, protected health information (PHI), which is held by or on behalf of health plans, healthcare clearinghouses and certain healthcare providers. Individually identifiable health information collected or generated by other entities is not protected by HIPAA, and since its passage in 1996, the volume of such information has grown exponentially. Today vast quantities of such data are collected by non-HIPAA entities, and the rapid development of technology, including health apps and other new technologies that generate, track and analyze such data, will only result in increasing amounts of health data falling outside HIPAA over time. The Confidentiality Coalition believes that it is imperative that this information be afforded privacy and security protections on a par with those of HIPAA. As stated in the Coalition's Beyond HIPAA Principles, a copy of which are attached, these standards should be national in scope, align with the definitions and concepts in HIPAA, and not disrupt the operations of HIPAA entities.

Non-HIPAA entities that hold or collect identifiable consumer health information have a responsibility to protect that information and use it appropriately. This includes requiring such entities to provide clear prior notice to consumers of the purposes for which they collect, use and transfer consumer health data, and to obtain consumer authorization for any other uses or disclosures. Individual authorization processes (including revocation of authorization) should be written in a meaningful and understandable manner and should be easily accessible to individuals. There should also be appropriate guardrails on the use of this data so that it may be used or disclosed for beneficial purposes, such as health research, in accordance with consumers' reasonable expectations. This will build consumer trust, which is essential to allow the use of their data for beneficial public policy purposes, including public health and medical innovations. As with other powerful technologies, artificial intelligence can be leveraged in ways that can bring enormous advances in medicine, such as to accurately diagnose diseases, or it can be used in ways that discriminate against and harm consumers if risks aren't appropriately mitigated. It is important that any privacy and security standards achieve the right balance to encourage and facilitate the former while preventing or reducing the risk of the latter.

As the FTC notes, lax security practices can result in great harm to consumers, and privacy standards are meaningless unless coupled with reasonable and appropriate safeguards. The Confidentiality Coalition recommends that security standards be risk-based, taking into account the size and complexity of the organization and the nature of the security risks and vulnerabilities arising from its operations. Given the heightened risk of cybersecurity attacks with respect to health data, organizations should be encouraged to adopt strong cybersecurity standards by allowing a safe harbor or enforcement discretion when an entity has adopted recognized security practices, similar to Public Law 116-321 enacted in 2021 with application to HIPAA entities. Finally, federal agencies should coordinate cyber incident and ransomware reporting requirements so that organizations are not subject to multiple or duplicative reporting requirements.

The Confidentiality Coalition appreciates this opportunity to provide comments to the FTC on the ANPR. Please contact me at tgrande@hlc.org or at (202) 449-3433 if you have any questions or seek more information about the comments in this letter.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large, looped "O" and a long, sweeping underline.

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