

October 21, 2022

April Tabor
Secretary, Federal Trade Commission
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Dear Secretary Tabor,

On behalf of the 30 member companies of the Electronic Health Record (EHR) Association, we are pleased to offer our comments to the Federal Trade Commission (FTC) on the Trade Regulation Rule on Commercial Surveillance and Data Security advance notice of proposed rulemaking (Commercial Surveillance ANPR, R111004).

As a national trade association of EHR developers, Association member companies serve the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs and other health IT across the United States, including by supporting the numerous practices they have adopted to secure sensitive patient information. Together, we work to improve the quality and efficiency of care through the adoption and use of innovative, interoperable, and secure health information technology. Although the FTC's ANPR covers a broad range of consumer data protections, our response will focus on aspects specifically pertaining to the protection of health information.

The HIPAA Privacy Rule provides federal protections for protected health information held by Covered Entities, but was not designed to accommodate the current landscape where actors other than Covered Entities, such as consumer apps, have health information in their stewardship. As a result, there is fragmentation in the expectations of stewards of health information depending on the context in which they operate, despite consumers believing their information is subject to HIPAA-like protections regardless of whether the actor holding their health data is a Covered Entity. The EHR Association strongly encourages the FTC to adopt rules that address this gap by establishing baseline expectations for the protection of consumer health information for commercial data stewards that are not already regulated by HIPAA. In doing so, FTC should avoid introducing duplicative privacy and security requirements for entities already regulated by HIPAA rules.

AdvancedMD	CureMD	Flatiron Health	MEDITECH, Inc.	Office Practicum
Allscripts	eClinicalWorks	Foothold Technology	Medsphere	Oracle Cerner
Altera Digital Health	eMDs – CompuGroup Medical	Greenway Health	Modernizing Medicine	Sevocity
Athenahealth	Endosoft	Harris Healthcare Group	Netsmart	STI Computer Services
BestNotes	Epic	MatrixCare	Nextech	TenEleven Group
CPSI	Experity	MEDHOST	NextGen Healthcare	Varian – A Siemens Healthineers Company

We offer the following considerations regarding the advanced notice of proposed rulemaking.

Sincerely,



Hans J. Buitendijk
Chair, EHR Association
Cerner Corporation



David J. Bucciferro
Vice Chair, EHR Association
Foothold Technology

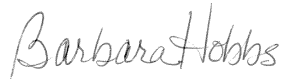
HIMSS EHR Association Executive Committee



Pamela Chapman
Experity



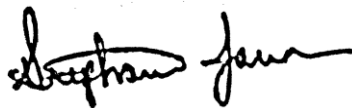
William J. Hayes, M.D., M.B.A.
CPSI



Barbara Hobbs
MEDITECH, Inc.



Cherie Holmes-Henry
NextGen Healthcare



Stephanie Jamison
Greenway Health



Sasha TerMaat
Epic

Established in 2004, the Electronic Health Record (EHR) Association is comprised of 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families. The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.

Electronic Health Record Association

Comments on the Federal Trade Commission (FTC) on the Trade Regulation Rule on Commercial Surveillance and Data Security advance notice of proposed rulemaking (Commercial Surveillance ANPR, R111004)

Which measures do companies use to protect consumer data?

HIPAA-regulated entities implement privacy and security programs to protect sensitive health information informed by risks specific to the individual organization. Examples of industry-recognized frameworks commonly utilized by healthcare organizations to secure protected health information include the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the International Organization for Standardization and the International Electrotechnical Commission ISO/IEC 27001, Statement on Standards for Attestation Engagements (SSAE) (SSAE 18 SOC2), and the HITRUST Cybersecurity Framework. Many cybersecurity best practices, however, are shared across cybersecurity frameworks or could be implemented independently of whether an organization adheres to a specific framework.

HIPAA-covered entities also rely on additional regulated programs and processes when establishing and implementing recognized security practices. Health IT certification requirements from the Office of the National Coordinator for Health Information Technology (ONC) include criteria for security, including requirements to support audit logging and tamper-resistance features that healthcare organizations might use as part of their efforts to ensure the security of protected health information. Additionally, healthcare organizations that electronically prescribe controlled substances are subject to security requirements from the Drug Enforcement Administration (DEA). Many also adhere to cybersecurity programs/frameworks used in the financial services sector, such as PCI Security Standards, in order to process payments from patients.

When defining policies in future rulemaking, the EHR Association strongly recommends that the FTC deem organizations as compliant with its rules if they design their privacy and security policies and programs to comply with HIPAA obligations.

Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?

HIPAA-regulated data should be protected regardless of which entity holds the data, but it should not be subject to duplicative regulatory frameworks for groups that are obligated to comply with HIPAA. Increasingly, however, there is an opportunity for PHI to move outside of the stewardship of HIPAA-regulated entities (e.g., consumer apps). Given the sensitive nature of health information, the EHR Association recommends that regulatory focus be given to actors who would collect or store PHI and are not currently regulated by HIPAA.

Should, for example, new rules require businesses to implement administrative, technical, and physical data security measures, including encryption techniques, to protect against risks to the

security, confidentiality, or integrity of covered data? If so, which measures? How granular should such measures be? Is there evidence of any impediments to implementing such measures?

HIPAA establishes and maintains an appropriate set of expectations for physical, administrative, and technical safeguards for protecting PHI in HIPAA-covered entities.

The EHR Association encourages the FTC to avoid excessively granular regulation. Instead, we suggest referring to industry standards and allowing organizations to design programs that appropriately address the scope and scale of their unique risks.

How do companies collect consumers' biometric information? What kinds of biometric information do companies collect? For what purposes do they collect and use it? Are consumers typically aware of that collection and use? What are the benefits and harms of these practices?

In the context of many consumer applications, biometric information identifies and authenticates individuals based on specific, recognizable, and verifiable unique data. However, it could also be interpreted to encompass health information that is routinely collected and used by healthcare providers, health plans, and their business associates to provide patient care or other healthcare-related services. The EHR Association urges the FTC to exercise caution when considering regulations on the use of biometric data, particularly in healthcare settings, as such limitations could yield unintended consequences that negatively impact their ability to provide patient care. FTC should specify in future rulemaking that biometric information will continue to be subject to HIPAA rules when actors are fulfilling the role of a Covered Entity or Business Associate as defined by those rules.

In addition to patient care, biometric data is commonly used to authenticate prescribers before transmitting prescriptions for controlled substances. The FTC will want to ensure that future rules do not inhibit the ability of healthcare providers to continue to use electronic tools to care for patients.

To what extent, if at all, should the Commission limit companies that provide any specifically enumerated services (e.g., finance, healthcare, search, or social media) from owning or operating a business that engages in any specific commercial surveillance practices like personalized or targeted advertising? If so, how?

Future regulations might impact the ability for public health agencies or others to engage in with public interest activities that often are required by the government, such as public health surveillance. The FTC should exempt restrictions on surveillance if the activity is for the purpose of reporting to a government agency or to fulfill an obligation required by law.