Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
January 15, 2022

Suresh Venkatasubramanian  
Assistant Director  
Office of Science and Technology Policy  
Executive Office of the President  
Eisenhower Executive Office Building  
1650 Pennsylvania Avenue  
Washington, D.C. 20504

RE: Connected Health Initiative Response to the Request for Information  
Regarding Public and Private Sector Uses of Biometric Technologies

I. Introduction and Statement of Interest

We write on behalf of ACT | The App Association’s Connected Health Initiative¹ (CHI) to provide comments to the Office of Science and Technology Policy (OSTP) on past deployments, proposals, pilots, or trials, and current use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes including individual mental and emotional states.²

CHI is the leading effort by stakeholders across the connected health ecosystem to clarify outdated health regulations, encourage the use of remote monitoring (RM), and support an environment in which patients and consumers can see improvement in their health. This coalition of leading mobile health companies and stakeholders urges Congress, the Administration, specialized agencies including the Office of the National Coordinator for Health IT (ONC), the Food and Drug Administration (FDA), the Centers for Medicare & Medicaid Services (CMS), and other regulators, policymakers, and researchers to adopt frameworks that encourage mobile health innovation using interoperable data while keeping sensitive health data private and secure. CHI supports OSTP’s timely effort to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or may be, impacted by their use or regulation.

² 86 FR 56300.
Care providers and patients (and others) who rely on innovative digital health products and services expect their valuable data is kept safe and secure, particularly their sensitive biometric data. The digital health community CHI represents practices and promotes responsible and efficient data stewardship to solve problems identified across consumer and enterprise health use cases. Patients, as well as stakeholders throughout the healthcare value chain, have strong data security and privacy expectations, and, as such, ensuring that the data collection and use practices reflect those expectations by utilising the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity. CHI recognizes that privacy and security are a shared responsibility, and we serve as a leading resource in the biometrics and privacy space for thought leadership and education for the digital health ecosystem.

CHI recognizes the specific subsets of biometric data described by OSTP are the focus of this request for information. However, we strongly urge OSTP to recognize that the use of patient-generated health data (PGHD), which includes biometric data, is integral to the future of the American healthcare system. The demonstrated benefits of the monitoring and timely action on PGHD include reduced hospitalizations and cost, avoidance of complications, and improved care and satisfaction, particularly for the chronically ill. For example, the Department of Veterans Affairs provides a compelling use case for the use of virtual chronic care management, which ultimately resulted in a substantial decrease in hospital and emergency room visits. Emerging technologies like telemedicine tools, wireless communication systems, portable monitors, and cloud-based patient portals that provide access to health records are revolutionizing RM and asynchronous technologies. Healthcare providers will also benefit from the potential of cost savings as a result of great responsible use of PGHD. Monitoring of PGHD demonstrably improves patient engagement dealing with chronic and persistent diseases to improve the management of such conditions.

Further, CHI urges OSTP to support the use of health data and PGHD through artificial intelligence (AI) in research, health administration and operations, population health, practice delivery improvement, and direct clinical care. The Administration’s policies should contribute to the investment in building infrastructure, preparing personnel and training, as well as developing, validating, and maintaining AI systems with an eye

toward ensuring value, ultimately offering a pathway for the voluntary adoption and integration of AI systems throughout the care continuum.

We believe OSTP shares CHI’s vision of a seamless and interoperable healthcare ecosystem that leverages the power of PGHD, including biometric data, and can be realized through the trusted framework. Providers of health plans and the beneficiaries they serve now expect access to seamless and secure patient data across the care continuum, where “[i]ndividuals are able to seamlessly integrate and compile longitudinal electronic health information across online tools, mobile platforms and devices to participate in shared decision-making with their care, support and service terms.”\(^6\) We support, and urge new policy activities related to this request for information to align with, parallel efforts by this Administration to develop the trusted framework for the responsible use of PGHD, including but not limited to:

- ONC’s development of an Interoperability Roadmap and PGHD framework;
- CMS’ continued efforts to support and pay for tools in Medicare that leverage PGHD, and to advance important changes to the future value-driven Medicare system which will permit caregivers to incorporate PGHD into how they coordinate care and engage with beneficiaries; and
- The FDA’s collaborative efforts to develop a governance framework for AI tools that meet the definition of a medical device under the Food, Drug & Cosmetic Act.

Notably, utilizing new and improved technology to ensure the confidentiality, integrity, and appropriate accessibility of data, such digital health tools allow for greater fraud and abuse detection, and would be of immense benefit to the Drug Enforcement Agency’s electronic prescribing of controlled substances (EPCS) program. Further, the ongoing COVID-19 public health emergency (PHE) has necessitated reducing in-person contact as much as possible, which the EPCS program can assist with for those legally prescribed controlled substances. CHI believes the DEA should reduce the regulatory burdens associated with its biometrics requirements, especially those that ignore advancements in technology and have kept costs unnecessarily high for those who electronically prescribe controlled substances. These regulations currently prevent innovators, and particularly small business innovators, from participating in the EPCS market. For example, the capability exists today for iPhones to provide a biometric factor (e.g., fingerprint or face scan) as a first authentication, with a software application installed on the same phone providing a separate and distinct authentication (e.g., a soft token). Sadly, such a scenario is prohibited by DEA’s interim EPCS rules with no discernable public benefit. CHI encourages reform to the EPCS program and urges the Administration’s consideration of detailed CHI recommendations provided directly to the DEA.\(^7\)

\(^6\) ONC, *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap* at 73.

\(^7\) [https://www.regulations.gov/comment/DEA-2010-0010-0157](https://www.regulations.gov/comment/DEA-2010-0010-0157).
II. Responses to the Request for Information

OSTP’s request for information (RFI) asks for input regarding two separate, but related categories of biometric technologies: 1) biometric recognition, which includes verification (one-to-one biometric matching) and identification (one-to-many queries that match an individual input against a larger database); and 2) biometric inference of cognitive and/or emotional states, such as mood or attentiveness. Below, CHI includes some findings on the two categories.

Biometric Recognition

Digital health innovators currently leverage numerous innovative biometric-assisted technologies, including facial verification, in order to provide services patients need and demand in the digital economy. Facial verification involves the comparison of a baseline, or “gallery”, image against another image, the “comparison” or “probe” image, sometimes provided by the consumer’s own device or by a device managed by the entity carrying out the comparison. Facial verification technologies are most often used for security purposes, i.e., to verify whether a person really is who they say they are. To share one key use-case, innovators currently use facial verification technologies embedded at the platform level, such as Apple’s Face ID, to allow users to log-in to apps using a scan of their face from the camera app. An app developer can choose integrate Apple’s Face ID as an option for users to select as one of the factors in a two-factor authentication scheme. For example, users often opt for two-factor authentication to improve device security in cases where an application stores sensitive personal information, such as bank account information. The mathematical representation of the individual’s face (the gallery image) used to validate the comparison image is stored within Apple’s Secure Enclave on the device and is not available to the developer, Apple, or any other third party.8

In recent years, academic and media reports have questioned the ethics and efficacy of various facial recognition technologies.9 Often those reports discuss facial identification, the sub-set of facial recognition technologies that match an individual against a much larger database of images and which have struggled with accuracy rates, bias, and

questionable deployment strategies.\textsuperscript{10} Facial verification currently programs, by contrast, are much more limited in scope and typically prove highly-reliable in testing. In its most recent Facial Recognition Vendor Test, the National Institute for Standards and Technology (NIST) found that the highest performing facial verification algorithms can achieve accuracy rates as high as 99.97 percent.\textsuperscript{11} While those accuracy rates tend to drop when the image collection occurs in less controlled environments (for example, verification via cameras in a crowded airport terminal), collection for a use-case like Face ID is typically well-controlled. Notably, many facial identification algorithms also perform increasingly well on recent NIST tests, some showing marked improvements over just the past few years since the negative reports first surfaced. In its latest assessment of facial identification algorithms, NIST concluded that “at least 30 developers’ algorithms outperformed the most accurate algorithm from late 2013.”\textsuperscript{12}

As the underlying technology continues to improve, digital health innovators are likely to implement a greater variety of facial recognition use-cases. Therefore, it will become increasingly important that regulation ensure that appropriate governance and accountability structures attach to each use-case commensurate with its risk. For example, in existing risk frameworks created by academics, targeted use of facial verification algorithms on a one-to-one basis typically represents a lower risk deployment, whereas real-time deployment of facial identification in public spaces is among the highest.\textsuperscript{13}

CHI supports legislation to limit particularly risky uses of facial recognition technology and consistently advocates for a federal privacy law that would limit how companies can process consumer data without their consent,\textsuperscript{14} and believes that a cross-sectoral risk-based framework for privacy will allow for the appropriately heightened steps to be taken for more sensitive data, including biometric data. Crafting rules that differentiate between targeted, consent-based uses of biometrics versus drag-net applications will be an important task for regulators going forward.


\textsuperscript{11} \url{https://pages.nist.gov/frvt/html/frvt1N.html}

\textsuperscript{12} \url{https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf}

\textsuperscript{13} Claire Garvie, Alvaro Bedoya, and Jonathan Frankle, “The Perpetual Lineup: Risk Framework”, Georgetown Center Privacy & Technology, October 18, 2016, \url{https://www.perpetuallineup.org/risk-framework}

Biometric Inferences of Cognitive or Emotional States

The collection of biometrics, including inputs that relate to or can infer cognitive or emotional states, holds both great promise and risk as one element in broader efforts to improve the quality of patient care in the United States. CHI seeks to advance responsible pro-digital health policies and laws that can harness the great potential of connected healthcare devices and tools, some of which may leverage biometric inputs, to unlock a higher standard of care for patients while minimizing potential harms.

One of the most exciting potential benefits of connected health technology is the ability of wearable devices that capture biometrics to improve equitable outcomes in healthcare. As co-creator of the Health Equity and Access Leadership (“HEAL”) Coalition, a group comprising about 35 organizations spanning the health ecosystem, CHI recently co-released a report highlighting how wearable devices, among other innovations, can contribute to reducing the divides in health outcomes across racial lines. As the report points out, access to traditional healthcare facilities, often stratified along income and racial lines, remains one of the major social determinants of health. The remote collection of health data through wearables can help ameliorate some of those disparities in access by allowing personalized diagnostics to occur outside of traditional healthcare institutions. For example, fitness trackers that collect valuable data, such as sleep patterns, activity and stress levels, can automatically share relevant information with clinicians, therapists, or coaches so that they can use granulated data to create more personalized care routines without requiring an in-person visit.

Connected health technologies that make use of biometrics to recommend cognitive or behavioral changes have shown efficacy in a number of different contexts to-date. For example, a trial of a mobile phone application that creates personalized behavioral interventions, including behavioral coaching, to improve for blood glucose control resulted in “substantially reduced glycated hemoglobin levels over 1 year.” The WellDoc mobile diabetes management platform also showed statistically significant improvements in A1c, in part due to behavioral recommendations. Some studies have also shown significant mental health improvements among users of certain mental health apps, depending on the level of engagement of the user.

In light of the COVID-19 pandemic, many turned to digital health platforms, tools, and services to consult with caregivers in greater numbers as in an effort to avoid the risk of exposing themselves or others to the virus. Wearable ownership and use increased in 2020, with 43 percent of respondents using wearables in 2020, compared to 33 percent

See Appendix 1.

16 https://diabetesjournals.org/care/article/34/9/1934/38702/Cluster-Randomized-Trial-of-a-Mobile-Phone
in the year prior. Additionally, during the COVID-19 public health emergency, more than half of all owners and users of wearables reported using them to manage a diagnosed health condition. 62 percent of physicians reported in a recent study that they believe wearable devices would increase the overall quality of care for their patients.

Clearly, usership of technologies that can pull biometrics and infer cognitive or emotional states will continue to increase, especially as efficacy improves and the benefits become clearer to users. CHI is keenly aware of the need to create appropriate guardrails to keep up with the growth of the industry and to ensure that mobile health players that collect sensitive biometric data continue to do so responsibly. Aside from advocating federal privacy legislation, as mentioned earlier, CHI continues to lead in advocating for the development of frameworks that will responsibly support the development, availability, and use of such AI innovations, including by developing Good Machine Learning Practices specifically for AI development and risk management of AI, as well as targeted recommendations on how to improve transparency for caregivers and patients.

---

20 Ibid.
21 https://vitalconnect.com/5-key-attributes-medical-wearables-seeking-adoptions-hospitals/
22 The CHI’s good machine learning practices for FDA-regulated AI are available at https://bit.ly/3gcar1e.
III. Conclusion

CHI strongly supports risk-based guardrails around the use of biometrics that provide consumers and patients with a baseline level of trust and that set a clear set of expectations for the businesses that seek to do good through these services. While the technology offers incredible potential, we understand the risks of misuse are particularly high in this context.

We thank OSTP in advance for its consideration of our views, and we look forward to engaging further in the future.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Matt Schwartz
Policy Associate

Leanna Wade
Policy Associate

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005
INTRODUCTION

Disparities in health are a long-standing issue in the United States due to the complex intersection of race, poverty, education quality and access, as well as the urban and rural divide. These disparities do not only affect the individuals and communities experiencing the disparities. They also impact overall health and well-being, and result in higher costs for health care across the country. The issue is particularly relevant today given the increasing diversity of the U.S. population coupled with worsening health outcomes in the country more broadly as compared to other developed nations.¹

Not all people living in the United States have the same opportunities to pursue a healthy lifestyle and that people of color, people with disabilities and those living in rural and low-income areas often have worse health outcomes.

This is largely due to access barriers to high-quality health care and social determinants of health ("SDOH").

Social determinants of health are conditions in the environments in which people are born, live, learn, work, play, worship and age that affect health and quality-of-life outcomes and health risks.² Inequities in factors like education, financial stability and food security are all driving forces behind the health disparities that exist in the United States today.

For instance, income tracks closely with health outcomes. Although Blacks and Hispanics have higher rates of disease overall than non-Hispanic Whites, these differences are “dwarfed by the disparities identified between high- and low-income populations within each racial/ethnic group.”³ Blacks, Hispanics and American Indian/Alaska Native people with higher incomes have better health than those with lower incomes.

The impact of income disparities is reflected in health outcomes. Residents of high-poverty areas (county poverty rate less than or equal to 20%) have a life expectancy of 76.7 years – 6.2 years shorter than the life expectancy for the residents of low-poverty areas (county poverty rate less than 5%). When stratified by gender, race and poverty level, life expectancy in 2012-2016 ranged from 71 years among Black men in high-poverty areas to 84.6 years among White women in low-poverty areas of the United States.⁴ Similar trends can be seen along the urban-rural divide and among those with and without a high school diploma.

SOCIAL DETERMINANTS OF HEALTH

Examples of social determinants of health:

- Availability of resources to meet daily needs (e.g., safe housing and local food markets)
- Access to educational, economic, and job opportunities
- Access to healthcare services
- Quality of education and job training
- Transportation options
- Public safety
- Social support
- Socioeconomic conditions like concentrated poverty and the stressful conditions that accompany it
- Access to mass media and emerging technologies (e.g., cell phones, the internet, and social media)
- Residential segregation
- Language/Literacy
- Social norms and attitudes like discrimination, racism, and distrust of government
- Exposure to crime, violence and social disorder
- Culture