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

Submitted Via Email: BiometricRFI@ostp.eop.gov

The White House
Office of Science and Technology Policy
1650 Pennsylvania Avenue
Washington, D.C. 20504

RE: Request for Information (RFI) Response: Biometric Technologies

Dear White House Representative:

Every American deserves the peace of mind of knowing that their personal health information is used appropriately and protected. For years, health insurance providers have supported this commitment, and that is why AHIP appreciates the opportunity to provide comments on the Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.

We provide information in response to the RFI about various health uses of these technologies, including by some health insurance providers. Our comments also address themes from the recently held OSTP Listening Sessions that sought public input on the future development of an Artificial Intelligence (AI) Bill of Rights to help avoid potential harmful consequences to individuals due to the use of biometric data.

AHIP applauds OSTP for taking a proactive approach to advance responsible AI for Americans. We will stay engaged as your office continues to explore the potential development of an AI Bill of Rights.

AHIP is the national association whose members provide health care coverage, services, and solutions to hundreds of millions of Americans every day. We are committed to market-based solutions and public-private partnerships that make health care better and coverage more affordable and accessible for everyone. With that experience and perspective, AHIP has been collaborating with public and private entities to lead the way in protecting consumers and advancing trustworthy AI. Our work includes:

- Participation with the U.S. Chamber of Commerce to develop AI principles for how American businesses serve consumers.
- Collaboration with the Consumer Technology Association in developing its new Trustworthiness Standard for AI in Health Care.
• Engagement with the National Association of Insurance Commissioners in their work related to the use of AI in insurance, mitigating bias in AI and pending Principles for Data Collection.
• Working closely on an ongoing basis with the Confidentiality Coalition to address AI policies and potential legislation and regulations.

Health Insurance Providers Use AI and Biometrics to Improve Care and Minimize Fraud

Health insurance providers currently use AI and biometric technologies to benefit patients and consumers, improving care and creating efficiencies while minimizing opportunities for fraud. However, we believe the full extent of the benefits of AI applications, including the use of biometric technologies within these models, have yet to be realized.

Some examples of how health insurance providers use AI include:

• **Clinical models** to understand health conditions through clinical research programs.
• **Predictive analytics** to identify patients who may benefit from improved access to services (based on metrics other than historical spending).
• **Physician performance** to identify high-value care for use in consumer choice and network design.
• **Service models** to enhance the customer experience.
• **Market research regarding prospective employer sponsors of health insurance** to help determine which employers might align with a company’s product offerings, value, areas of access, or health care networks.
• **Actuarial analysis** to help identify utilization patterns (not individually identifiable) for an employer or other health plan sponsor to understand usage trends both now and for the future.
• **Claims analysis** to identify potential fraud and abuse.

Additional examples that specifically highlight specific uses of biometric technologies in healthcare and by health insurance providers can include:

• **Voice biomarkers** to improve care by identifying patient needs, authenticating users, and detecting emergencies.
• **Clinical vocal biomarkers** for health tracking, detection and triage, as a diagnostic aid, risk prediction, to assess discharge readiness, and as a remote patient monitoring tool.
• **Voice recognition** to improve human-to-human interaction by capturing notes and supporting care teams (e.g., authorized user dictation). Combined with AI, voice recognition can leverage data from visits to provide care recommendations to providers (e.g., at the point of care in a health setting), as well as potentially expedite claims processing.
• **Clinical diagnostic data** with applied AI can augment the ability to pinpoint diseases, monitor conditions, and establish tailored care paths. For example, this may include genetic testing results in combination with clinical imaging using biomarkers for specific cancer types (i.e., detection and diagnosis) to assist with determining which therapies would be best suited for an individual.
• **Fingerprint and facial biomarkers** (i.e., retinal scans or facial recognition) can be appropriately applied to expedite authentication and access. For example, leveraging fingerprint or facial recognition technology, alongside user consent to use and transparency around such applications, to log into phones and devices to access information and programs can enable efficient authentication and access the person requesting access, such as consumers accessing their phone, plan members using a medical device, or provider-partners accessing medical platforms in a secure way particular to the individual.

• **Personal characteristics** captured in vision, audio and natural language processing models can aid in identifying conditions. For example, models can assess body language, gait, word choice, pupil dilation and other factors while an individual answers questions for an avatar or performs an action.

### Recommendations for Considering an AI Bill of Rights for Americans

• As AI continues to advance, we recognize there may be challenges and new areas to explore. Health insurance providers are seeking ways in which they can allow consumers to direct how their information is used, improve privacy and security, mitigate potential implicit data bias, establish governance best practices, and achieve other shared objectives. We recommend that as OSTP continues to consider the development of an AI Bill of Rights, future discussions should explore:

  • **Educating consumers about the uses of the technologies, along with the potential benefits and risks.** Consumers should know what AI is and how it is used in public and private sectors (e.g., how consumers will interact with and utilize AI-powered tools in different or intersecting sectors). **Consumers should also have resources on the benefits (e.g., privacy and security) and potential drawbacks that may be associated with some of those uses** (e.g., data breach, data scraping, loss of privacy, secondary uses of data). Americans will be more likely to trust AI-powered services if they can clearly obtain relevant information and benefit from its utility.

  • **Preventing harmful intended bias and taking actions to address potential unintended bias.** Depending on the application, understanding and being transparent about potential bias in AI is the first step toward mitigating unintended consequences. Context is crucial in determining how to address potential “bias” in the use of AI. For example, some AI initiatives are designed to benefit specific groups or populations, which might be considered “good bias,” even though the approach is deliberate and beneficial. In other words, we need to be able to distinguish between different approaches to ensure that important efforts to avoid harmful bias, do not impede deliberate and beneficial efforts to identify and benefit an underserved group or population. Engaging a diverse set of stakeholders who will be impacted by the AI in the design of the use cases is a good way to better understand AI programs, promote beneficial advancements, and mitigate harmful unintended outcomes as much as possible.

  • **Ensuring that governance programs, practices or procedures can be applicable to the context, scope, and data use of a specific use case.** AI efforts exist against an
important backdrop of existing laws. There may well be benefit from voluntary activities among industry participants, such as principles or best practices. Areas for such legal or potential industry guidance include: data privacy and consent, transparency that a biometric technology is being used and for what purpose, and the right for a user to opt out. Governance is essential for engaging public trust, a consistent framework across applications, and appropriate and ethical use of the technologies. Likewise, program design will be a key element for AI, as well as how automated and supported decision-making by AI directly relate to the key governance rules.

- **Focusing on consumer understanding and the effective use of the technology.** Public and private entity uses should be disclosed. Federal agencies, including the National Institute of Standards and Technology (NIST) and others can help inform new regulatory proposals, which should align with the work of OSTP. To date, NIST has been a federal leader in this area and should serve as a resource for individuals and entities as substantive and technical policies are developed and adopted.

- **Making policy makers and the public aware of the AI functions in current systems, and existing measures to ensure fairness and effectiveness throughout use and application.** We must balance benefits from AI against the associated risks and design policies that seek to mitigate those risks in a way that least interferes with beneficial innovation.

- **Staying ahead of foreign actors and governments** that attempt to leverage the technology to outpace the United States from a competitive standpoint or nefarious activities, and ensuring that foreign actors and governments, and U.S.-based public and private entities do not exploit the privacy and security of individuals.

The use of AI and biometric technologies hold great promise for improving health care for everyone. We can work together to address the challenges and ensure patients are protected while promoting innovation. Engaging a diverse set of stakeholders is essential to success, and AHIP and our health insurance provider members are eager to work with you and other stakeholders on these important efforts.

Please contact me at [ ] if you have any questions and for future engagement.

Sincerely,

Matthew Eyles
President & Chief Executive Officer