Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on Advancing Privacy Enhancing Technologies

AHIP

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

AHIP™
Guiding Greater Health

601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004

T 202.778.3200
F 202.331.7487
ahip.org

July 8, 2022

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

Sent Via Electronic Mail to: PETS-RFI@nitrd.gov

Re: Request for Information (RFI) Response: Privacy-Enhancing Technologies (PETs)

Dear White House Representative:

Everyone deserves the peace of mind of knowing that their personal health information is private and protected. With our long-standing commitment to protecting the health information of patients and consumers, AHIP appreciates this opportunity to submit comments on the Notice of Request for Information (RFI) on Advancing PETs.[1] **We support the development of a national strategy on privacy-preserving data sharing and analytics, along with associated policy initiatives.** Our comments and insights are based on health insurance providers' extensive experience in evaluating new technologies and best practices for consumer data privacy and security.

AHIP[2] members are accustomed to protecting the privacy and security of individuals' health information. While complying with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, State laws, and corresponding regulations, our members continually strive to institute best practices, add emerging technologies that meet or exceed the current legal and compliance expectations, and stay on the forefront of new developments and solutions to better protect their customers.

OSTP's evaluation can be important for privacy, security, and cybersecurity policies that serve as a significant "next step" in health care transformation by empowering data with technological protections that are based on our national values, individual rights, and the ongoing need to stay competitive with and ahead of advancements currently occurring in other countries and jurisdictions for economic and national security.

[1] 87 Fed. Reg. 35250.
[2] 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.

Given the importance of this initiative, as well as the breadth and scope of this work, we recommend the issuance of a proposed national strategy in the *Federal Register*, along with a focused outline of the components that are expected to be involved in the deployment and implementation. We believe that additional information from OSTP would allow for a more fulsome and substantive response addressing PETs based on OSTP's vision and plans.

A National Strategy for PETs

AHIP and our members are committed to supporting and advancing PETs. Yet, many stakeholders across the health care spectrum are in different places when it comes to their sophistication with these solutions and techniques. **The educating of stakeholders about a baseline set of terms and working definitions by OSTP would help further the discussions and focus on the issues to be encompassed in the national strategy.** We believe a subsequent opportunity to offer additional comments on these terms and working definitions would better inform the work and developments in this area for the national strategy.

There is also uncertainty about whether the RFI is intended to cover: (1) the ability of consumers to understand and manage their own choices based on privacy and control of individually identifiable and/or health data, and/or (2) the technological solutions and supporting policies that can foster anonymized data sharing, research, interoperability, and other needs utilizing enhanced privacy tools that inform data sets without compromising privacy and security on an individual basis. Clarifying the scope of the RFI in this regard can better inform future responses and allow for more relevant information to be offered.

Coordination of Efforts at the Federal Level

The Notice explains that the OSTP has been collaborating with several existing efforts, including the National Science and Technology Council's Fast Track Action Committee on Advancing Privacy-Preserving Data Sharing and Analytics, Subcommittee on Networking and Information Technology Research and Development (NITRD), the National Artificial Intelligence (AI) Initiative Office, and the NITRD National Coordination Office. We appreciate the coordination to minimize duplicative or misaligned policies and believe the public would benefit from more information about these efforts.

For example, the National Institute of Standards and Technology (NIST) has been working on several projects, including the development of a Privacy Framework, a Cybersecurity Framework, a Risk Management Framework for AI, and other test projects and pilot programs to further evaluate the use of technology solutions and the potential risks and benefits of advancing such solutions in the health care and other sectors. In public forums, NIST has described working with the OSTP, although it is currently unclear the extent to which NIST may be involved with PETs in this context.

In addition to NIST, other federal agencies are either charged with or are developing regulations and guidance to promote privacy, security, and cybersecurity. For example, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights, the HHS Office of the Coordinator for Health Information Technology (ONC), the Centers for Medicare & Medicaid Services (CMS), the Federal Trade Commission (FTC), and many other federal agencies have to date issued some form of privacy, security and/or cybersecurity guidance. **We support a comprehensive and collaborative federal approach that will help consumers and other affected stakeholders better understand which agencies are engaged in this work, as well as the direction and focus of OSTP in terms of collaboration and priorities by industry sector (i.e., healthcare, retail, financial, etc.). This information can help commenters understand how the national strategy and related PET policies may align with, duplicate, or conflict with existing federal laws, regulations, and guidance.**

For the health care sector specifically, short-term as well as long-term goals should be developed. For other sectors, priority should be given to the national critical infrastructure sectors to help stage the development of PETs and application in these sectors.

Discussion of Emerging Technologies

Many recent technologies can advance business processes and data sharing techniques while also improving how we protect individually identifiable data. In healthcare, examples of these technologies include, but are not limited to:

- distributed ledger and blockchain-based technologies.[3]
- confidential computing examples such as the "Zero-trust Frameworks" for security.
- federated learning.
- "web3" which may further enhance consumers' ability to control and restrict how their online data is used.
- "data sandboxes" which can offer a secure and governed environment in which certified de-identified health data is provisioned to vetted users.[4]

[3] Blockchain use in healthcare can address needs for improved data movement, such as payer-to-payer exchange, which requires secure communication and the ability to share data between different entities. See also an article which illustrates one member's efforts to test blockchain to improve efficiencies for Coordination of Benefits (COB) functions: https://www.forbes.com/sites/michaeldelcastillo/2022/02/08/forbes-blockchain-50-2022/?sh=14c9409f31c6.

[4] One example of a "data sandbox" can be found at: https://massdigitalhealth.org/mass-digital-health-programs/digital-health-sandbox-program/digital-health-sandbox-network/anthem.

- synthetic data.[5]

These tools – when applied appropriately – can reduce privacy and security issues surrounding the release personal and sensitive information while advancing opportunities to use data in a multitude of contexts, such as validating and training AI algorithms on substantial amounts of data. In addition, PETs will enable advancements across research, grant, and start-up programs for companies as well as other specialized projects. **OSTP could encourage advancement of PETs across these programs by exploring federal support of safe harbors, "data sandboxes," and demonstration projects.**

The health care industry can specifically benefit from understanding the goals and risks of PETs. Currently, much work is taking place to promote interoperability of health data on a national scale. This work is being conducted under the auspices of the HHS ONC, via a contract with The Sequoia Project, the Recognized Coordinating Entity for the Trusted Exchange Framework and Common Agreement (TEFCA). To the extent that PETs can further refine and protect data, this national initiative stands to benefit from such transformative work.

One result from fostering the greater use of PETs would be to allow healthcare consumers, providers and other entities to execute certain choices in an electronic environment based on consumer preferences and the ability of the provider or entity to share data. Preferences would need to be documented and executed, where feasible, but consideration should be given to those entities or individuals who are unable to execute such preferences perhaps because of patient safety or other concerns.

Furthermore, we strongly support use of PETs to advance research, particularly research that can benefit health outcomes, mitigate disease, help with early identification and treatment, and inform overall health and well-being. PETs that can help inform research and treatment outcomes are a key interest for consumers and our members. **The OSTP could encourage advancements specific to healthcare by supporting public-private collaborations and the use of PETs.**

It is also important to note that privacy cannot be discussed in a viable way without also considering security (as well as cybersecurity), as privacy and security go hand-in-hand to protect data and confidential information. Many PETs are built on the security infrastructure to protect data. **The focus of the RFI is currently on privacy but could be expanded to include security since PETs need the "what" of privacy controls and the "how" of security controls to be effective and work as intended.**

[5] A recent article highlights the opportunities of synthetic data in healthcare: https://www.wsj.com/articles/anthem-looks-to-fuel-ai-efforts-with-petabytes-of-synthetic-data-11652781602.

Building public trust and acceptance centered around privacy, security, and cybersecurity will be essential components for moving forward in diverse settings and applications as PETs are utilized. Such confidence can help promote national acceptance and adoption.

Legal Considerations

In terms of laws, regulations, and guidance, a comprehensive and diverse series of general resources are available, but many do not specifically address PETs. At this stage, we caution against prescriptive regulations focused on PETs. We believe it would be prudent to allow PETs to be utilized and understood before constructing regulatory requirements. Creating regulatory requirements too early may hamper innovations in this area.

As public and private entities are learning more about PETs and deploying them in health and other sectors, flexibility and innovation will be key to learning what works and what may need improvements. Laws, regulations, and guidance should be developed at a future point when appropriate.

International Collaboration and Standards

Privacy considerations cannot be discussed in the United States without prioritizing the rights that are afforded to all Americans. The work that is taking place in international venues may prove to have some societal benefits, but in the United States any benefits must be balanced against the risks to individual rights. It is expected that PETs will protect individually identifiable data. However, as we have learned from cybersecurity campaigns and data breaches, no electronic system can provide absolute assurances that the systems and the data will be immune from intrusion or compromise. More understanding of the risks involved in potential cyber campaigns and breaches and how such incidents could be handled in the international context would be needed before American consumers could be asked to trust such technologies and processes.

In addition, varying international efforts can create confusion and result in inconsistent schemes. Many countries and jurisdictions have priorities and values that differ from U.S. values and laws. Some of our members comply with U.S. laws and regulations, as well as the European Union’s Privacy Framework, the General Data Protection Regulation. Compliance with varying regulatory schemes is complex and can be costly to implement. **Within the confines of remaining consistent with U.S. rights and values, we encourage the OSTP to seek out ways to promote efficiency and reduce costs to benefit the health care consumer when data and PETs are used in international collaborations.**

We appreciate the opportunity to comment on this important topic. Please contact me at - with any questions.

Sincerely,

Danielle A. Lloyd
SVP, Private Market Innovations and Quality Initiatives