Comments of the World Privacy Forum
Regarding the Need for Increased Transparency, Communication, and Work on Vaccination Data Policy, including Restriction of Commercial Marketing use of Vaccine Data of Individuals

to

HHS National Vaccine Advisory Committee (NVAC) Meeting

September 14, 2021
via public comments and via email to NVAC@HHS.GOV

Chair Hopkins and members of the Committee, thank you for the opportunity to participate in the HHS NVAC meeting today. I am the founder and Executive Director of the World Privacy Forum. WPF is a non-profit public interest research group, and we have worked on privacy and data governance of complex ecosystems for more than two decades (www.worldprivacyforum.org). A major focus of our work includes issues regarding health data ecosystems, their governance, and attendant privacy interests.

We have three brief points today regarding the queries the Committee put forward in the September 14 meeting regarding 1) what additional areas the Committee should address; 2) what additional stakeholders should be involved; and 3) what research questions should be addressed.

I. A crucial additional area of work for this Committee is to a) create transparency around privacy and other policies relevant to identifiable vaccination data; and b) communicate vaccination data policy to all stakeholders

People who are already vaccinated and those who are not vaccinated have numerous questions and concerns about the processing (collection, use, disclosure, maintenance, and security) of identifiable vaccine data. The most common questions we are hearing include:

- What is being done with my vaccine data?
- Who else gets access to my information?
- What laws protect this data in digital proof of vaccination systems?
- Does HIPAA apply to vaccination data?

As members of the Committee know, the intersection between HIPAA privacy regulations and public health data is labyrinthine and messy at the best of times. But now, due to the extraordinary circumstances we find ourselves in during the pandemic, public health authorities have not yet focused on communicating to people about the broader processing of and protections for vaccination data. Protections for this data are important because the uncertainty around data utilization — especially in digital proof-of-vaccine systems — makes some members of the public nervous and undermines trust in the public health system. We see the work of articulating a clear and privacy-protecting policy for vaccine data both within and without public health authorities as an important next step for HHS to take soon. Both data subjects and data processors need clear statements about data usage.

The ACIP Committee already produced important initial work to help protect vaccine data from misuse. This work may be found in the CDC / ACIP *COVID-19 Vaccination Program Provider Requirements,* published May 18, 2021. These requirements specifically prohibit the use of vaccination data for commercial marketing purposes. We were pleased to see this prohibition stated overtly. This is the type of protection needed to ensure patient trust in the public health data ecosystem.

Specifically, the May 2021 CDC / ACIP *Vaccination Program Provider Requirements* asserts that **COVID-19 vaccination registration information** and **vaccine administration data** may not be used or disclosed for commercial marketing purposes or any other non-allowable purposes. The actual text of the CDC May 18, 2021 requirements regarding the marketing restriction states:

> "Use of Vaccine Recipient Data for Commercial Marketing Purposes Prohibited
>
> Notwithstanding uses or disclosures otherwise allowed by law, providers are prohibited from using or disclosing data collected from vaccine recipients for and through the CDC COVID-19 Vaccination Program for commercial marketing purposes or for any other purpose not allowed under this updated provision of the COVID-19 Vaccination Provider Agreement. Such data include COVID-19 vaccination registration information and vaccine administration data. These data are collected solely for the purposes of the CDC COVID-19 Vaccination Program and must be maintained in a manner that protects the integrity of the CDC COVID-19 Vaccination Program by only being used or disclosed for the purposes

of the COVID-19 Vaccination Program and other limited purposes that promote public health, advance positive patient outcomes, and promote health equity.

This prohibition is not intended to limit communications by health care providers to vaccine recipients with whom the provider has an existing relationship prior to contact about COVID-19 vaccination.

The following are not included in the above prohibition:

- Communications regarding receipt of a second dose, or potential booster dose(s), of COVID-19 vaccine
- Communications to vaccine recipient for public health purposes
- Communications to vaccine recipients involving pharmacy or clinical services of the provider, personalized to the vaccine recipient's medical needs, even if those services are not directly related to COVID-19 vaccination
- Availability of other vaccines (e.g., shingles, pneumococcal conjugate, seasonal influenza, routine childhood vaccines)
- Clinical emails
- Disease screening services
- Communications about the availability of programs to manage particular health conditions (e.g., asthma, diabetes, heart disease)

In addition, de-identified, aggregate datasets can be used by providers and shared with other partners for public health, population health, and health equity purposes.

Communications with COVID-19 vaccine recipients involving the store component of any pharmacy or other provider participating in the CDC COVID-19 Vaccination Program are considered prohibited commercial marketing. For example, text, e-mail, mail, or other communications to COVID-19 vaccine recipients about products on sale in the store are prohibited as commercial marketing.

COVID-19 vaccination registration information and vaccine administration data collected in the course of participation in the CDC COVID-19 Vaccination Program cannot be sold, for direct or indirect remuneration, even with permission of the vaccine recipient."
https://www.cdc.gov/vaccines/covid-19/vaccination-provider-support.html (5/18/21).

We note that standard HIPAA rules already prohibit health care providers and health plans from using or disclosing patient data for commercial purposes. We emphasize the importance of the

CDC requirement that expressly prohibits someone in the vaccination infrastructure (e.g., a merchant operating a HIPAA hybrid entity, like a supermarket with a pharmacy), from using vaccination information for any inappropriate purpose outside the hybrid entity.

II. Extend the prohibition on the use of vaccine recipient data for commercial marketing purposes to "proof of vaccine" systems

We urge the Committee to advise ACIP to ensure that the same prohibitions already in place regarding commercial marketing use of vaccination data should also be mandated for any digital or other vaccine credentialing system (proof of vaccination or proof of a negative COVID-19 test). We see significant risks for the commercial marketing use of patient registration and vaccination data due in part to the sheer number of digital proof of vaccination systems in development across complex public-private pathways.

We note that when proof of vaccination status is no longer voluntary, the calculus for privacy changes. There is a potential forthcoming OSHA emergency regulation that will set terms for employers and vaccinations, which will likely create broader needs to create and use proof of vaccination systems. In this broader context, we urge additional mandatory requirements on how that data can be used. It is still unknown how many cities, schools, or workplaces will require proof of vaccination status. Just to identify one such effort as an example, the city of San Francisco announced mandatory proof of full vaccination in certain indoor venues.

There are rapid developments in COVID-19 vaccine data systems, such as the build out of the Vaccine Administration Management System (VAMS), the upgrading of the Immunization Information System (IIS), and now a new ecosystem of vaccine credentialing subsystems. There should be no place or opportunity in this new ecosystem for the commercial marketing use of vaccine recipient data.

We note here a separate but related issue regarding overall questions and misunderstandings about health surveillance systems and their functions, including well-established pharmacosurveillance systems. Public health authorities understand that vaccination information is part of broader public health surveillance programs and systems, with the term "surveillance" used specifically in the health context. But the public may not have this same nuanced understanding of the use of the term "surveillance" in the health context. Public health surveillance systems should be made very transparent to vaccine recipients, with greater clarity of how the data is utilized. Beyond this, proof of vaccination systems put in place to address the pandemic must not be permitted to create new types of public health surveillance systems applicable beyond public health purposes.

III. We recommend including patient and privacy stakeholders to assist with policy inputs and communication strategies

One of the questions NVAC asked during the meeting focused on which stakeholders needed to be brought into the conversation. In order to increase transparency, trust, and solve problems that patients are concerned about, we urge the Committee to engage with patient groups and privacy and data experts in order to learn what the data and privacy concerns are so as to create appropriate policy guardrails for vaccine data held outside of HIPAA and outside of the public health system. Soliciting input from these stakeholders will surface concerns and help HHS craft effective solutions.

We recognize the challenges here, and we also recognize the legitimacy of the concerns. We believe that this Committee can arrive at good solutions that allow for appropriate data use while appropriately restricting data processing.

To conclude, we support the work of HHS and this Committee to protect patient privacy interests and the integrity of public health data. We request and urge the Committee to extend protections to vaccine recipient data as that data starts to move into the rapidly developing, multiple, and in some cases overlapping vaccine credentialing systems and proof of vaccine tools and apps.

There is much to be said in how vaccine credential systems should operate. This Committee has the ability to make the most important statement of all about this ecosystem: that the data of vaccine recipients is protected, and credentialing systems utilizing that data are prohibited from utilizing that data for commercial marketing or other unauthorized purposes.

Thank you for the opportunity to participate today. I welcome your questions.

Respectfully,

Pam Dixon,
Founder and Executive Director,
World Privacy Forum
www.worldprivacyforum.org