PERSONALIZED MEDICINE COALITION

April 7, 2025

The Honorable Brett Guthrie
Chairman
Committee on Energy & Commerce
U.S. House of Representatives
2161 Rayburn House Office Building
Washington, DC 20515

The Honorable John Joyce, M.D.
Vice Chairman
Committee on Energy & Commerce
U.S. House of Representatives
2102 Rayburn House Office Building
Washington, DC 20515

Re: Privacy Working Group Request for Information

Dear Chairman Guthrie and Vice Chairman Joyce:

The Personalized Medicine Coalition (PMC), a multi-stakeholder group comprising more than 200 institutions from across the health care spectrum, thanks the House Committee on Energy & Commerce for the opportunity to provide information on parameters of a federal comprehensive data privacy and security framework.[i] We believe it is important for any federal data privacy legislation to consider the complex and unique uses of data in health care, where the use and disclosure of such data is already subject to many existing federal statutes and regulations. PMC's comments provide recommendations for how federal legislation can support the continued flow of data and information critical to personalized medicine research and health care delivery, while protecting the privacy of individual health information.

Personalized medicine is a rapidly evolving field in which physicians use diagnostic tests and individual details about a person and their health to determine which medical treatments will work best for each patient or use medical interventions to alter molecular mechanisms that impact health. By combining data from diagnostic tests with an individual's medical history, circumstances, and values, health care providers can develop targeted treatment and prevention plans with their patients.

Personalized medicine is helping to shift the patient and provider experiences away from trial-and-error toward a more streamlined process for making clinical decisions, which will lead to improved patient outcomes, a reduction in unnecessary treatment costs, and better patient and provider satisfaction. PMC and its members are leading the way in personalized medicine and in developing evidence showing how patients and the health care system can benefit from appropriate testing and tailored treatment as soon as possible during their clinical experiences.

Statement of Neutrality

PMC's members may present their own responses to the Committee on Energy and Commerce's *Privacy Working Group Request for Information* and actively advocate for those positions. PMC's response is designed to provide feedback so that the general concept of personalized medicine can advance, and is not intended to impact

adversely the ability of individual PMC members, alone or in combination, to submit separate responses to Congress on this request for information.

Recommendations for a Federal Data Privacy Framework Advancing Personalized Medicine

In recent decades, health care has been transformed by the ability to analyze massive amounts of data to inform prevention, diagnosis, and treatment. Advances in our understanding of the human genome have provided an important new window into the unique biological attributes of an individual, and their impact on health. In addition to patient data created within health care systems and leveraged through electronic health records (EHRs), health data are now widely attainable from consumer sources such as health apps, wearable devices, home health monitoring devices, and patient reports. Combined with the widespread adoption of digital technologies and information sharing, multiple data sources can now contribute to a broader and deeper understanding of disease and a patient's health. Progress in personalized medicine depends on protecting individual patient privacy while making this data available for research and health care delivery.

Building on PMC's 2022 report *Using Health Data to Advance Personalized Medicine: Challenges and a Path Forward*,[ii] PMC encourages Congress to consider the following recommendations for a federal comprehensive data privacy and security framework. Several charts from the report are included as appendices.

1. **Federal privacy legislation should pre-empt state laws regarding data privacy and/or artificial intelligence.**
   In recent years, a patchwork of state privacy laws and regulations has emerged, creating compliance challenges for health care entities that operate in multiple states. Duplicative and conflicting state and federal regulations hinder the aggregation of data, research, and sharing of health information. Conflicting regulations could limit, for example, patients' access to clinical trials and essential therapies emerging from multi-state, multi-center research programs. Federal pre-emption of state laws around data privacy, including state laws regarding data privacy in the context of artificial intelligence, is critical to mitigating this fragmented approach to privacy protections and aligning requirements across states.

2. **Federal privacy legislation should preserve standards already adopted under HIPAA.**
   In 1996 through the *Health Insurance Portability and Accountability Act (HIPAA)*, Congress enacted a regulatory structure for enabling essential uses of data for health care delivery, administration, and research while protecting the privacy of patients. Existing HIPAA Privacy and Security Rules govern the use, disclosure, confidentiality, integrity, and availability of protected health information (PHI), or information that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service. Appendix I enumerates HIPAA and subsequent federal legislation governing access to and protection of health data. Preserving standards already adopted under HIPAA will ensure that HIPAA-covered entities across the health care system can continue to operate smoothly.

3. **HIPAA should serve as the baseline for any additional federal standards enacted around health information, including consumer-generated health information.**
   Data generated by consumers through mobile apps, commercial genetic testing companies, financial records, and wearable digital health devices are not protected under HIPAA. Appendix

II illustrates sources of health data and the regulatory divide that currently exists between HIPAA protected and non-HIPAA protected data. While consumer generated data has value to health care research, it also creates new privacy exposure for patients. Federal legislation could consider opportunities to clarify the applicability of existing HIPAA requirements to certain contexts, such as artificial intelligence and privacy and security requirements for non-PHI data that may be used by such applications. Using HIPAA as a baseline for any additional standards around health information would limit disruption to HIPAA-covered entities, where federal privacy protections are already implemented and well-understood.

4. **To avoid unintended disruptions, federal privacy legislation must consider how entities currently operate and use data in the context of health care.**
   The flow of data across organizations conducting health research, developing clinical-support tools, and delivering care is highly complex. For example, many clinical laboratories operate as hybrid entities under HIPAA – meaning that they may conduct functions that make them HIPAA covered entities, as well as other functions not governed by HIPAA, which may or may not be regulated separately by other federal laws. Therefore, even if federal legislation were to exempt HIPAA-covered entities from the applicability of new data privacy requirements, legislation could still impact hybrid entities, including many clinical laboratories. To avoid any unintended consequences, Congress should consider the impacts of any new requirements on hybrid entities.

   In addition, previous legislation under consideration in Congress proposed data retention policies by "categories of data" (e.g., financial information, health information, genetic information). This approach was at odds with existing data storage and retention practices in health care, which are often developed based on the "type of record" (e.g., test orders, claims reimbursement). We encourage Congress to continue to consult stakeholders to assess the implications of any federal privacy legislation on health care.

5. **Federal legislation should preserve the existing HIPAA framework governing the use of de-identified data in health research.**
   The availability, use, and sharing of de-identified health information is critical to conducting research that advances our understanding of disease, the discovery of new interventions, and their evaluation on patients' health outcomes. Standards for de-identification of data have been established by the *HIPAA Privacy Rule*. Under this framework, once data is de-identified, it is no longer considered PHI and researchers are permitted to use and share data with other researchers and organizations without violating patient privacy. Additional protections have enabled genetic information to become more widely available for personalized medicine research and treatment, including the *Genetic Information Nondiscrimination Act (GINA).* GINA prohibits discrimination based on genetic information with respect to health insurance and employment, with subsequent related regulations prohibiting discrimination in access to health care based on predisposition to inherited diseases.

   Combined with GINA protections, the existing HIPAA framework for the use and sharing of de-identified health data is key to facilitating personalized medicine research. This includes efforts like the All of Us™ Research Program led by the U.S. National Institutes of Health (NIH) and launched in 2018 to collect genetic and health information from one million volunteers as part of a decades-long research project. Making data broadly accessible for research purposes while upholding data privacy and security are core tenets of the program. Ultimately, the program will

enable new discoveries through the identification of risk factors and biomarkers that allow more efficient and accurate diagnosis and screening, more rational use of existing treatments, and the development of new treatments.

Federal privacy legislation establishing limitations on the transfer of data between entities should not hinder sharing de-identified data for health research purposes. In addition, when transferring de-identified data to a third party not covered under HIPAA, the third party should be the entity held responsible for maintaining de-identification. Federal privacy legislation can avoid unintended disruptions to health research by preserving existing HIPAA standards governing the sharing of de-identified data and PHI, which apply to genetic information and to certain real-world health data collected from sources outside of traditional clinical trials.

6. **Federal legislation should not impede the ability of patients, providers, clinical laboratories, and other health care entities from using or sharing health information to facilitate treatment, payment, health care operations, or legal obligations.**
Previous legislation under consideration in Congress would require patient consent for data transfers between entities, including genetic information. In general, PMC supports efforts to empower patients with control over their health data, which includes the ability to easily access their own health data, decide who to share it with, and honoring patient choice, so long as it is not inconsistent with the obligations or capabilities of providers. Future standards must continue to ensure an appropriate level of privacy for all health data to maintain trust in the research and health care delivery process. New data privacy requirements, however, should not impede the sharing of a patient's health information between health care providers and/or other entities for the purposes of informing clinical decision-making and the delivery of care, especially when sharing PHI for treatment, payment, and health care operations purposes is already facilitated under HIPAA. Any new consent requirement for the use and disclosure of PHI could jeopardize the provision of personalized medicine by entities such as clinical laboratories that are typically not in a position to obtain consent because they are indirect providers. The timely return of genetic test results, for example, from a clinical laboratory or a diagnostic testing company to a patient and their provider is critical to informing clinical decision-making, helping patients experience better health outcomes, and delivering personalized medicine. Likewise, where a health care provider is legally obligated to retain records of PHI for a certain period of time, or to disclose it to government officials for public health or law enforcement purposes, no individual right of control of the data that would be inconsistent with those obligations should be established.

Conclusion

PMC appreciates the interest of the Committee on Energy and Commerce's Privacy Working Group in examining parameters of a federal comprehensive data privacy and security framework. We look forward to working with you to ensure that any such framework supports the continued flow of data and information critical to personalized medicine research and health care delivery, while protecting the privacy of individual health information. If you have any questions about the content of this letter, please contact me at cbens@personalizedmedicinecoalition.org, or David Davenport, PMC's Director of Public and Science Policy, at ddavenport@personalizedmedicinecoalition.org.

Sincerely,

Cynthia A. Bens
Senior Vice President, Public Policy

Appendix I: US Legislation Governing Access to and Protection of Health Data[iii]

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA, enacted in 1996, established national standards to protect sensitive patient health information (protected health information, or PHI) and defined requirements for patient consent to share information. It set the stage for information interoperability by requiring the government to establish code sets, unique identifiers, and operating rules for electronic transactions. HIPAA addresses security standards and enforcement actions for breaches in covered information systems to protect against nonconsensual use of data.

Genetic Information Non-discrimination Act (GINA)

The 2008 GINA prohibits discrimination based on genetic information with respect to health insurance and employment. Subsequent related regulations prohibit discrimination in access to health care based on predisposition to inherited diseases.

The Affordable Care Act (ACA)

The 2010 ACA broadened insurance coverage and promoted the use of electronic transactions for payment and information sharing.

Health Information Technology for Economic and Clinical Health (HITECH) Act

The 2009 HITECH Act offered financial incentives for provider organizations to adopt electronic health information technology and enacted privacy and security requirements for the transmission of health information, with penalties for non-compliance. The law included federal investments in infrastructure, payment incentives, and regulatory penalties to hospitals and providers that did not comply.

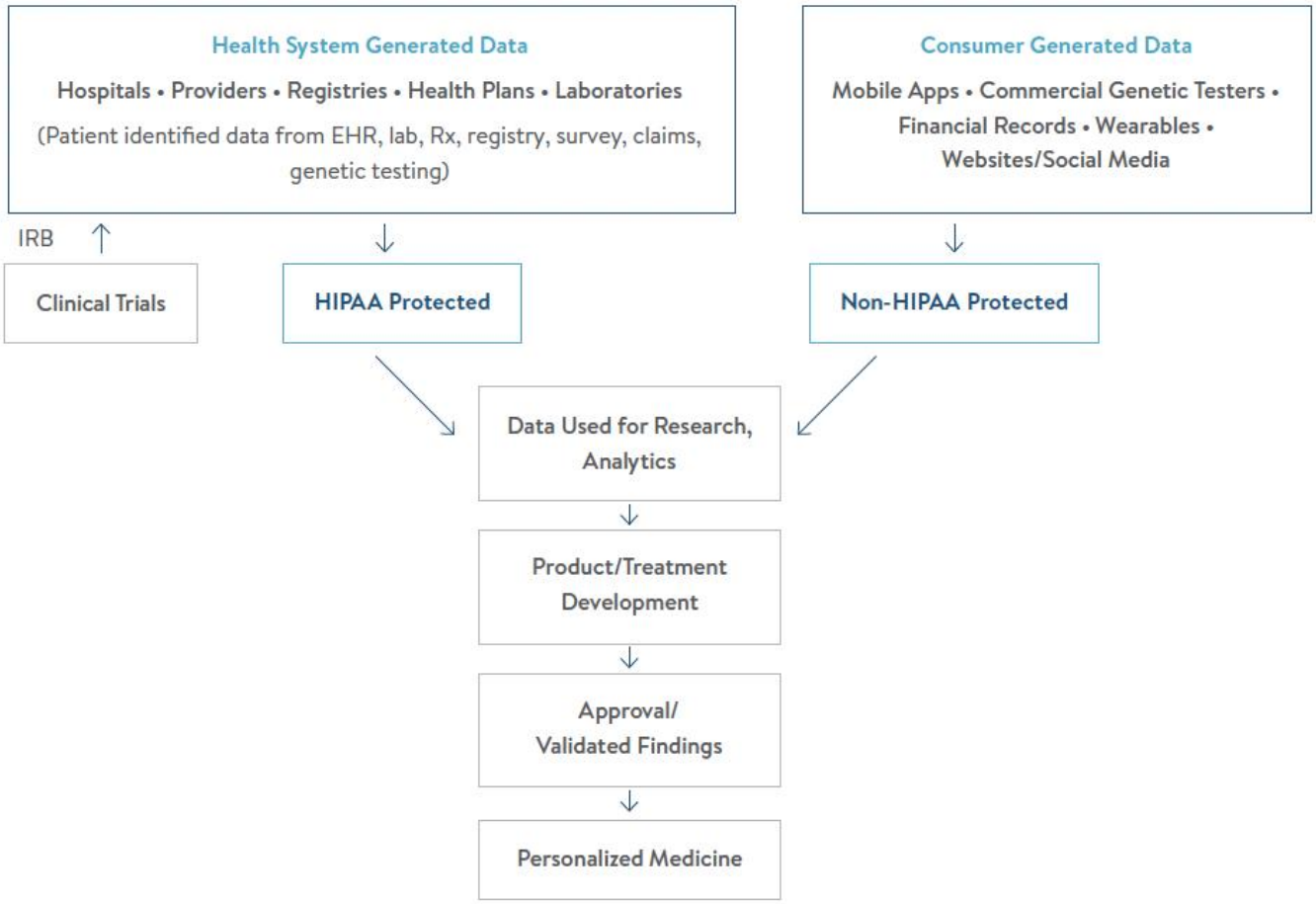
The Medicare Access and CHIP Reauthorization Act (MACRA)

MACRA in 2015 built on earlier legislation requiring adoption of electronic health information systems and created a plan to achieve interoperability. It also adopted a payment system that required quality reporting and action towards interoperability for Medicare providers.

21st Century Cures Act (Cures Act)

The Cures Act of 2016 accelerated personalized medicine by addressing bottlenecks in the access to and use of data. Major revisions in policy were implemented to overcome "information blocking" and improve interoperability.

Appendix II: Privacy Protections for Personal Data Contributing to Personalized Medicine[iv]



[i] U.S. House Committee on Energy & Commerce. *Privacy Working Group: Request for Information*. February 12, 2025. https://d1dth6e84htgma.cloudfront.net/02_21_2025_PWG_Request_for_Info_2_e1753e1356.pdf. (accessed March 25, 2025).
[ii] Personalized Medicine Coalition. *Using Health Data to Advance Personalized Medicine: Challenges and a Path Forward.* 2022. https://www.personalizedmedicinecoalition.org/Userfiles/PMC-Corporate/file/Using_Health_Data_to_Advance_Personalized_Medicine_Challenges_and_a_Path_Forward.pdf. (Accessed April 1, 2025).
[iii] Personalized Medicine Coalition. *Using Health Data to Advance Personalized Medicine: Challenges and a Path Forward.* 2022. https://www.personalizedmedicinecoalition.org/Userfiles/PMC-Corporate/file/Using_Health_Data_to_Advance_Personalized_Medicine_Challenges_and_a_Path_Forward.pdf. (Accessed April 1, 2025).
[iv] Personalized Medicine Coalition. *Using Health Data to Advance Personalized Medicine: Challenges and a Path Forward.* 2022. https://www.personalizedmedicinecoalition.org/Userfiles/PMC-Corporate/file/Using_Health_Data_to_Advance_Personalized_Medicine_Challenges_and_a_Path_Forward.pdf. (Accessed April 1, 2025).