Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Dear Ms. MacFarland:

Thank you for providing the public with the opportunity to provide comments on the request for information (RFI) entitled "Developing a Privacy Framework," 83 FR 64531 (November 14, 2018). The Centers for Medicare and Medicaid Services (CMS) is aware that the public comment period ended on January 14, 2019, during a partial shutdown of the Federal government. While we were not able to respond at that time, we would like to offer a few, brief comments. We predict these will be consistent with the interests of many other Federal agencies, and with other feedback you will receive.

As I'm sure NIST is aware, privacy is a significant priority for CMS. CMS handles a tremendous amount of personally identifiable information (PII), and some of the PII CMS collects, holds, and uses is subject to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, and is therefore also protected health information (PHI). Every year, nearly 40 million individuals receive services through Medicare, delivered by over 1.2 million providers. CMS maintains records of Medicare-eligible individuals, Medicare recipients of services, individual health care claims, providers, and its own employees. CMS must implement privacy and security controls that affect all of these data sets, including those required by the HIPAA Privacy and Security Rules; the e-Government Act (including the Federal Information Security Modernization Act (FISMA)); the Privacy Act of 1974; provisions of the Affordable Care Act (ACA); and many more. CMS has additional privacy and security interests in Medicaid transactions. While almost all Medicaid data is collected and used at the state level, CMS provides guidance to state-level contractors and agencies. Protecting patient privacy is therefore extremely critical to meeting CMS's mission and ensuring public trust in our agency.

Several of the questions posed to stakeholders in the RFI related to existing standards, frameworks, models, methodologies, tools, guidelines, best practices, and principles that may be most relevant and useful to organizations with privacy interests **(e.g., Questions 10-13, 18, and 26)**. When identifying sweeping privacy concerns that may affect an entire organization or subunit's infrastructure, staff, business processes, or missions, CMS continues to value the Fair Information Practice Principles (FIPPs). While other conceptions of privacy may provide novel insights or innovations, CMS believes the FIPPs continues to define the scope and content of

any robust institutional privacy program. While perhaps the most well-known version of the FIPPS originated in 1973 (US Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens* (1973)[1]), CMS has found that the expansion and refinement of the FIPPs developed by the Organization for European Cooperation and Development more thoroughly addresses modern information Privacy concerns (OECD, *OECD Privacy Framework* (2013)[2]). The FIPPs has persisted over decades in framing the basic concerns of a privacy program that holds data concerning consumers of services, those affected by the activity of government agencies, and many other stakeholder groups. We predict that NIST will find it most convenient to organize and scope its Privacy Framework by relying on a current and comprehensive version of the FIPPs.

Many other questions posed to the public in the RFI asked about major challenges or concerns in protecting the privacy of data subjects **(e.g., Questions 1, 2, and 19-25)**. CMS's major privacy-specific concern relates to the issue of transparency. Many laws and regulations require CMS to provide data subjects with clear and comprehensive information concerning what data CMS and its business partners collect; how that information is used; how data subjects may receive copies of information pertaining to themselves; and what other rights they may have related to records and other data held by CMS. CMS continuously seeks new and better ways to communicate its mission and activities to the public, while complying with existing privacy-related requirements. CMS's activities include some that occur at most (or even all) civil agencies, including developing public notices such as systems of records notices (SORNs) and Privacy Impact Assessments (PIAs); developing and updating websites to inform the public of CMS's privacy policies and procedures; communicating with members of the public that request access to their own records and/or corrections and updates to these records; and ensuring privacy information is included in handbooks and other materials made available to beneficiaries and enrollees. Whereas many other privacy interests are treated as shared responsibilities between privacy and security professionals, the promotion of transparency is a privacy-specific activity requiring a large percentage of our available resources.

Other questions in the RFI related to issues of constraints or parameters of a Privacy Framework **(e.g., Questions 10-12, 16, and 19-25)**. CMS is subject to many laws and regulations, including those listed above, and continues to be very attentive to NIST policies and guidance mandated by the e-Government Act, most notably NIST's Special Publication 800-53 (*Recommended Security Controls for Federal Information Systems and Organizations*). While CMS will follow developments related to the Privacy Framework with great interest, CMS's first priority remains implementing risk management and compliance activities that comply with existing requirements. We will be very interested to see how the Privacy Framework may inform or structure these existing obligations.

[1] Available at https://aspe.hhs.gov/report/records-computers-and-rights-citizens.
[2] Available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Once again, CMS is grateful to NIST for undertaking this important project. We look forward to participating in future workshops and discussions.

Respectfully,

Michael Pagels
Director, Division of Security, Privacy Policy, and Governance
(DSPPG) Acting CMS Senior Official for Privacy (SOP)