January 4, 2021

The Honorable Seema Verma
Administrator,
Centers for Medicare & Medicaid Services
U.S. Department of Health and Human Services
7500 Security Boulevard
Baltimore, MD 21244-1850

Re: Medicaid Program; Patient Protection and Affordable Care Act; Reducing Provider and Patient Burden by Improving Prior Authorization Processes, and Promoting Patients' Electronic Access to Health Information for Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, and Issuers of Qualified Health Plans on the Federally-facilitated Exchanges; Health Information Technology Standards and Implementation Specifications (CMS-9123-P)

Dear Administrator Verma:

The Confidentiality Coalition appreciates the opportunity to submit comments on the proposed rule issued by the Centers for Medicare & Medicaid Services (CMS)and the Office of the National Coordinator for Health Information Technology (ONC).

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective patient confidentiality protections. The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

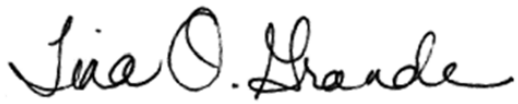
The Confidentiality Coalition supports efforts to improve interoperability and promote the electronic exchange of health care data, including giving patients access to prior authorization information to better manage their care, while reducing the burden on the healthcare system. Improving these efforts will not only reduce provider burdens but give patients greater access to their health information. We encourage CMS and ONC to ensure that any regulatory changes to improve interoperability are consistent with existing privacy and security frameworks under HIPAA. Robust privacy protections are necessary to ensure that greater interoperability and data sharing is conducted in a safe and sustainable way that does not sacrifice patient privacy. The proposed rule would require a greater level of information sharing among patients, providers and other stakeholders. It is important for these efforts to recognize the potential

privacy challenges in sharing additional patient information, particularly with entities not subject to HIPAA, and work with stakeholders to ensure these concerns are properly addressed. Ensuring patient trust is an important step in promoting interoperability, particularly regarding data not covered by HIPAA protections. A recent survey found that 90% of participants voiced concern with the privacy of health data not protected by HIPAA.[1] It is important for these patients to have trust in the safety of their data to receive necessary participation in promoting data sharing.

Regarding the Request for Information on giving patients greater control over their health information and data segmentation, we support giving patients greater control over the sharing of their health information with third parties, but are also mindful that without complete health records, patient care and access to care may be jeopardized. Therefore, it is critical that CMS and ONC strike the appropriate balance between allowing patients to limit sharing of their sensitive health information and the need for accurate and complete health records to deliver and coordinate patient care. We would welcome the opportunity to provide further comments and information on this important topic.

The Confidentiality Coalition looks forward to working with CMS and ONC to improve patient access to information while protecting privacy of health information. Attached is a copy of our 'Beyond HIPAA' principles that serves as a framework for sharing health information. Please feel free to contact Tina Grande at 202-449-3433 or tgrande@hlc.org.

Sincerely,



Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council

[1] Ben Moscovitch, *Americans Want Federal Government to Make Sharing Electronic Health Data Easier*, The Pew Charitable Trusts (September 16, 2020), https://www.pewtrusts.org/en/research-and-analysis/articles/2020/09/16/americans-want-federal-government-to-make-sharing-electronic-health-data-easier.

Beyond HIPAA Privacy Principles

1. For the last 20 years, the HIPAA Privacy and Security Rules have engendered public trust that individually identifiable health information collected by providers and insurers (HIPAA covered entities) would be disclosed only for health functions like treatment, payment processing, and safety, and not used or disclosed for other purposes without an individual's authorization. Any future legislation or rulemaking that addresses individually identifiable health information should not conflict with HIPAA's Privacy and Security Rules.

    a. HIPAA's required "Notice of Privacy Practices" provides an overview of individuals' rights as well as permitted and required uses and disclosures of identifiable health information.

    b. HIPAA's approach requires use of risk-based administrative, technical, and physical safeguards allowing organizations the flexibility to implement policies and controls commensurate with the level of risks they have identified.

2. Congress should establish a single national privacy and security standard for *all* health information *not* subject to HIPAA. This single standard:

    a. Should not conflict with HIPAA,
    b. Should not disrupt day to day practices for HIPAA Covered Entities and Business Associates,
    c. Should align with HIPAA's definitions of health information, and
    d. Should adopt a risk-based approach for the development and implementation of security and privacy controls like HIPAA.

3. Individuals may not fully appreciate that individually identifiable health information collected outside of a HIPAA Covered Entity or Business Associate Agreement are not afforded HIPAA privacy and security protections. Individuals should be given clear, succinct notice concerning collection, use, disclosure, and protection of individually identifiable health information that is not subject to HIPAA.

4. Individual authorization processes (including revocation of authorization) for use and disclosure of identifiable health information not covered by HIPAA should be written in a meaningful and understandable manner and should be easily accessible to individuals prior to and after information is used or shared.

Effective date: May 2020

5. Entities that hold or collect identifiable health information have a responsibility to take necessary steps to maintain the trust of individuals. Entities that are not HIPAA Covered Entities or Business Associates that hold identifiable health information should clearly stipulate the purposes for which they collect, use, and disclose identifiable health information.

6. For data use and activities other than the purpose for which the data was provided, individuals must provide authorization for collection and use of individually identifiable health information. Such information collected, used or disclosed by entities outside of HIPAA should be limited to only that information needed to accomplish the purposes for data collection. This practice provides privacy protection while allowing for continued innovation.

7. Individuals should be informed of their right to seek redress – from the entity and from regulators – in the case of unauthorized access, misuse, or harm attributable to how their identifiable health information was collected, used or disclosed.

8. Penalties and enforcement must be meaningful in order to discourage misuse and unpermitted collection, use or disclosure of identifiable health information.