March 10, 2023

The Honorable Chiquita Brooks-LaSure
Administrator
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244
Mail Stop: C4-26-05

RE: Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Advancing Interoperability and Improving Prior Authorization Processes for Medicare Advantage Organizations, Medicaid Managed Care Plans, State Medicaid Agencies, Children's Health Insurance Program (CHIP) Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, Merit-Based Incentive Payment System (MIPS) Eligible Clinicians, and Eligible Hospitals and Critical Access Hospitals in the Medicare Promoting Interoperability Program (CMS-0057-P)

Dear Administrator Brooks-LaSure:

The Confidentiality Coalition appreciates the opportunity to submit comments on the proposed rule to advance interoperability and improve prior authorization.

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, and others, committed to advancing effective health information privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security 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 thanks the Centers for Medicare and Medicaid Services (CMS) for their work to improve information sharing among healthcare stakeholders. Providing relevant healthcare information on a timely basis helps patients to better manage and understand their care. As CMS continues to support policies that advance health information sharing, we ask the agency to ensure that protecting patients' privacy remains a priority. Leveraging patient application program interfaces (APIs) reduces barriers to information sharing, but with this greater access to patient information comes increased risk to the privacy and security of that data.

It is imperative that CMS ensure that there are appropriate safeguards to protect patient data every step of the way from the health plan to the patient. A single incident involving the misuse or diversion of patient data could undermine the interoperability paradigm envisioned by CMS by eroding the patient trust that has been built up over decades under the HIPAA framework. As we emphasized in our comments with respect to the CMS Interoperability and Patient Access Final Rule, third party applications selected by patients are often not subject to the Health Information Portability and Accountability Act's (HIPAA) Privacy and Security Rules. This is because many of these applications are not offered by or on behalf of covered entities, but rather, are offered directly to the patient. Many patients do not fully appreciate that the protections of HIPAA do not extend to these applications, and that the security of their health data is entirely dependent on the privacy and security practices adopted by their chosen app.

While it is important that patients be informed that their health information, once accessed by a health app on their behalf, is no longer protected by HIPAA, this alone is not sufficient. Patients do not have the means or expertise to impose or properly evaluate privacy safeguards adopted by the health apps that they choose to use. Rather than imposing the primary responsibility for ensuring that these health apps have appropriate privacy and security practices on patients themselves, we believe there are other more effective measures that CMS can take within the limits of its authority to help protect patient data that flows from HIPAA covered entities through the Patient API to non-HIPAA third party health apps.

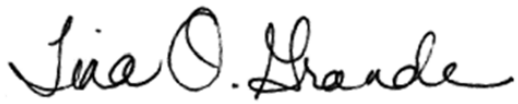
One such measure, as suggested by CMS, is to require that any non-HIPAA entity acting on behalf of a patient to access their data through the API become an Individual Access Service (IAS) Provider under the Trusted Exchange Framework and Common Agreement (TEFCA). By becoming a signatory to TEFCA, the entity will be agreeing contractually to privacy and security measures substantially the same as those required of HIPAA entities. To overcome any regulatory authority issues, CMS could provide that impacted payers may condition registration of an app for access to the Patient API on the app providing evidence that it is a signatory to TEFCA as an IAS Provider. This will provide more substantive and meaningful protections for patient data than measures that require disclosure by the app of its privacy policies, since as CMS itself has noted, disclosure does not in itself ensure minimum privacy and security standards.

Another important safeguard that CMS can implement is to allow impacted payers to require health apps to provide verification that they are authorized by the patient to access the patient's protected health information. A valid HIPAA authorization to disclose the PHI to a third party is already a HIPAA requirement, but impacted payers should also be permitted to impose reasonable verification requirements to ensure that the app is not only clearly authorized by the patient, but also that the app is who it says it is and is transparently acting on the patient's behalf. This is particularly important in this context, given the ease with which data may be accessed through the Patient Access API, and the nature and volume of data available, both of which provide opportunity and incentive for unauthorized bad actors to seek to gain access to patient information. Many times, such bad actors gain access by asserting that they are acting on the patient's behalf even when this is not the case, or where they have used deceptive practices such that the patient did not understand or fully appreciate what was being agreed to.

Ultimately, impacted payers should be given sufficient flexibility to ensure that any APIs being used to advance interoperability do not expose patients to unnecessary privacy or security risks.

The Confidentiality Coalition looks forward to working with CMS on steps to improve interoperability while maintaining patient privacy. Please contact me at tgrande@hlc.org or 202-449-3433 with any questions.

Sincerely,



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