The American College of Obstetricians and Gynecologists
WOMEN'S HEALTH CARE PHYSICIANS

Vice President, Health Policy
Barbara S. Levy, MD
email: blevy@acog.org

June 14, 2019

Alex M. Azar II
Secretary
Department of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue, SW
Washington, DC 20201

Donald W. Rucker, MD
National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C St SW, Floor 7
Washington, DC 20201

Re: Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2

Dear Secretary Azar and Dr. Rucker:

On behalf of the American College of Obstetricians and Gynecologists (ACOG), representing over 58,000 physicians and partners dedicated to advancing women's health, I am pleased to offer these comments on the second draft of the Office of the National Coordinator for Health Information Technology's (ONC) Trusted Exchange Framework and Common Agreement (TEFCA). We believe this is an important part of the effort to exchange health information and further advance interoperability to improve care quality and coordination across our health care system. However, it is imperative that the privacy and security of patients' health information is protected throughout this process. We look forward to working with ONC to build a more interoperable health IT ecosystem that better addresses and prioritizes women's unique health needs while reducing administrative burden on physicians.

ACOG applauds ONC for encouraging public input, incorporating comments received on Draft 1 of TEFCA in 2018, and providing an additional opportunity for public comment. TEFCA has significant implications on the privacy and security of patients' health information. Although ONC aims to dramatically increase the accessibility of patients' electronic health information (EHI), there are not enough proposed provisions to protect this valuable, sensitive information. While we agree that the ability to easily share information will improve care coordination and reduce unnecessary duplication of tests and other services, the risk of patients' health information being inappropriately shared will also increase substantially. In the absence of policies that require electronic health record (EHR) and app developers to take steps to protect patients, developers are unlikely to implement privacy and security features into their products. Patients may withhold sensitive clinical information from their ob-gyns and other health providers once they determine they cannot control what is being shared across the health care system. We believe it is ONC's responsibility to ensure that health IT regulations preserve the provider-patient relationship. **Data segmentation at the element level is critical for protecting patient privacy in an interoperable system. ACOG strongly urges ONC to improve access and affordability of data segmentation software for all providers.**

Security Labeling

ACOG applauds ONC for incorporating a significant number of comments requesting efforts be focused on addressing security labeling, especially for sensitive, protected data. Currently, security labels can be placed on data to enable an entity to perform access control decisions on EHI but only at the highest level (document or security header). Providers are not able to tag data elements for privacy or keep track of which elements patients have consented to sharing and which they have not. We understand ONC's strategy to limit the proposed security labeling requirement to commonly requested data categories, as the Data Segmentation for Privacy (DS4P) Implementation Guide has yet to reach wide adoption, but ACOG strongly believes data segmentation is essential for the protection of women's (and others') EHI, and we support a more granular approach.

Certain notes and data elements specific to women's health should not be released unless specific permission from the patient is obtained. For example, segmenting data at the element level would protect individuals who have experienced intimate partner violence, sexual assault, and other sensitive experiences that disproportionately affect women and other at-risk populations. This would also allow ob-gyns and other health providers to maintain confidentiality of documentation related to care for sexually transmitted infections (STIs), pregnancy, substance use disorder, mental health conditions, or other conditions that, if shared, could endanger women or make them more vulnerable to discrimination. Patients are likely to withhold sensitive clinical information from their ob-gyns and other health providers once they determine they cannot control what is being shared across the health care system or that they cannot prevent certain EHI from being shared with a spouse or caregiver.

Data segmentation and consent management software currently exist, but these functions are costly to implement in many EHRs and are not accessible to all providers or practices. Further, ACOG is concerned that patient data protections and privacy controls are an afterthought in software design and development. ONC should work with CMS, EHR developers, and other stakeholders to make data segmentation technologies accessible and affordable to all providers, including independent and small practices. Mechanisms to monitor and control data access, patient consent and privacy, and ensure data provenance, governance, and enforce state and federal law must be inherent in EHR development. As it becomes easier to share data, ACOG believes it is imperative that granular data segmentation standards be included in the TEFCA.

Although ACOG believes data segmentation is essential, we are sympathetic to ONC's approach to limit the security labeling requirement to commonly requested sensitive data categories—such as SAMHSA Consent2Share sensitivity value sets for mental health, HIV, and substance abuse, and the EHI of minors—in the interim period before wide adoption of DS4P. Due to the current limitations of data segmentation software, this practice could be very burdensome for providers, and antithetical to ACOG and ONC's efforts to reduce provider burden. Having a pre-defined format for sensitive elements could be an effective solution to protecting sensitive EHI without increasing provider burden, until the appropriate technology allowing documenting providers, in conjunction with the patient, to label individual elements as secure, is widely available. To that end, we recommend the following be added as a sensitive data category and labeled as secure: intimate partner violence, sexual assault, STIs, and elective abortion. ACOG again urges ONC to ensure that granular data segmentation technology is accessible to all providers, including pediatric and women's health providers. We strongly believe that, as EHI is shared more freely, the capability to segment data will become increasingly important, and the

appropriate technologies should be developed in a way that will not increase the administrative burden of providers.

ACOG Recommendations:

- That documents and information collected on intimate partner violence, sexual assault, all STIs – not limited to HIV, and elective abortion make up an additional sensitive data category and labeled as secure.
- Ensure that data segmentation software is affordable and accessible to all providers, including independent and small practices.