June 17, 2019

Don Rucker, M.D.
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

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

Dear Dr. Rucker:

On behalf of Imprivata, we thank you for the opportunity to provide comments on TEFCA Draft 2. We believe that, with further calibration, TEFCA can be the vehicle to achieve the fundamental interoperability required to enable value-based care: that no matter where a patient appears in the care continuum, providers will be certain who the patient is, can confidently access the correct records from previous episodes of care, and can easily update the right record, for subsequent use by other providers.

Imprivata is uniquely qualified to help inform the Administration's work to achieve interoperability. Based in Lexington, Massachusetts, for the last seventeen years, our 460 employees have worked to provide 1,945 healthcare organizations around the world with an industry-leading trusted digital identity platform to address critical compliance and security challenges while improving provider productivity and the patient experience.

In reviewing TEFCA Draft 2 in conjunction with the 21st Century Cures Act; Interoperability, Information Blocking, and the ONC Health IT Certification Program (RIN:0955-AA01); CMS Interoperability and Patient Access (RIN:0938-AT79), Imprivata has concluded that:

1. *The transition to valued-based care currently underway must continue and accelerate*. Federal spending on Medicare and Medicaid, amounting to just over $1 trillion in 2016, and growing faster than the US economy, is not sustainable.
2. *Value-based care is impossible without interoperability*. Across a distributed and often unaffiliated care continuum, patients and providers need to be able to confidently access an accurate, complete medical record in order to support prevention of illness, manage chronic conditions, and decrease the need for hospitalization. Trusted and efficient access to protected health information (PHI), both past and recent treatments, across the care continuum is necessary for effective and timely delivery of care. With clear trusted patient identity, and the use of technology, we can arm providers with a complete history of events, diagnosis, treatment and medications, substantially curtailing or eliminating re-testing and

associated incremental costs. This enables our providers to access and leverage current and past PHI to accelerate and improve the diagnosis process, reduce re-admissions, and deliver a superior level of service to the patient.

3. *Interoperability is impossible without positive patient identification*. No matter where a patient appears in a care continuum, before previous records can be accessed, before matching algorithms can be invoked, certainty about who the patient is must be established. The method to achieve positive patient identification is already well-established. NIST Special Publication 800-63-3, Digital Identity Guidelines, a standard promulgated by the Department of Commerce, provides a logical approach to every aspect of the management of digital identities, balancing the degree of security and certainty required against the level of risk associated with misidentification.

We have a specific recommendation which we believe will enhance the impact and effectiveness of TEFCA.

TEFCA Draft 2 cites NIST 800-63-3 as applicable for purposes of supporting requests by Individual Users (i.e. patients) to access their electronic health information (EHI). TEFCA Draft 2 requires that QHINs (paragraphs 6.2.4 - 5), Participants (i.e. provider organizations, see paragraphs 7.9 - 10), and Participant Members (i.e. health care professionals, see paragraphs 8.9 - 10) identity proof patients at NIST Identity Assurance Level 2 (IAL2), and authenticate them at NIST Authentication Level 2 (AAL2).

We fully support the application of NIST identity proofing and authentication standards to provide certainty and security to the processes used to support patients seeking access to their records (i.e. Individual Access Services). However, more importantly, at least the same level of certainty and security should be applied to the care process (i.e. Treatment). Identifying patients with certainty and security at every encounter in the continuum of care should be a fundamental practice in healthcare, for reasons related to both patient safety and to provide the interoperability necessary to support value-based care. Conceptually, TEFCA Draft 2 supports this view, in that both Treatment and Individual Access Services have been maintained as Exchange Purposes. We encourage ONC to make this very explicit: the identity proofing and authentication standards required by TEFCA Draft 2 for Individual Access Services should also be required to support Treatment. **We suggest ONC add "Patient Identity Management" as an Exchange Purpose, and require the application of NIST 800-63-3 identity proofing and authentication standards for that purpose in a 5 step approach:**

1. *Conduct robust identity proofing at the first patient encounter (i.e. enrollment), or at the shortest possible time thereafter, to confirm a patient is who (s)he claims to be*. The identity proofing process confirms that a unique, valid identity exists -- and verifies that the valid identity belongs to the patient claiming it. Identity proofing to IAL2 can be done as it is today, in person by patient access staff at a provider's facility.

   Technologies exist to identity proof patients to IAL2 online; these could be deployed to support innovations to improve patient access to care, by extending positive patient identification further in the continuum of care, e.g. to enroll a new rural patient at his / her first telehealth encounter. The same technologies could be deployed on-site in existing healthcare kiosks, for the sake of enabling patient self-enrollment and reducing the burden on provider patient access staff.

Whether in person or online, demographic data elements related to identity (name, address, phone number, …) and any applicable unique identifiers (Medicare ID, VA ID, SSN, …) could be discovered and validated, **establishing a foundational trust anchor for all subsequent healthcare transactions**.

2. *Perform an initial record search.* Having performed robust identity proofing to establish a trust anchor, immediately search on that basis to **determine what historical records may exist across the provider organization's care continuum**. Capture the associated medical record numbers (MRNs) as additional attributes of the patient's identity.
3. *Complete enrollment by issuing appropriate authenticators to patients, so that identity proofing does not have to be repeated each time a patient returns for care*. An authenticator is something the patient possesses and controls, which is used to confirm the patient's identity (i.e. affirms connection to the trust anchor). Authenticators consist of something the patient has, knows, or is. The most common authenticator, historically, has been a password (i.e. something the patient knows).

   Imprivata believes the use of appropriate authenticators will be particularly impactful toward achieving interoperability, because:

   a. Authenticators provide the best method for convenient, secure communication of high quality, up-to-date (see Step 5 below) demographic data elements and unique identifiers for all appropriate healthcare transactions, eliminating transcription and data entry errors.

   b. Authenticators can be deployed so that when used, connection to the right record for the care location where the patient has presented is automatic. **When used in this way, the creation of duplicate records and entry of patient data into the wrong record (an "overlaid" record) are prevented**.

   c. The use of authenticators advances the ideal of establishing one patient identity across the healthcare continuum, which is the foundation for achieving interoperability.

   The best authenticators are some combination of "has," "knows," and "is" that:

   a. Meet or exceed NIST AAL2 requirements.

   b. Cannot be used without the represented patient's permission (i.e. can't be stolen or faked).

   c. Are accurate, i.e. a non-enrolled patient is not mistaken for an enrolled one, and an enrolled patient is not mistakenly rejected.

   d. Are easy for patients to use.

   e. Require minimal maintenance (e.g. don't require re-enrollment, or resets, as is the case with passwords).

   Imprivata believes strong biometric authenticators are especially useful for healthcare, because they:

   a. Meet the criteria immediately above.

   b. Are preferred by patients. In June 2017 and January 2018, The Pew Charitable Trusts worked with Public Opinion Strategies and Hart Research Associates to conduct 11 focus groups with 95 participants in five cities, and reported that "biometrics were the most

frequent first - or second - choice solution, not only among the different types of unique identifiers, but all proposals. Focus group participants preferred this option because it would help unconscious patients, not need to be remembered by the patient, and be more accurate and secure than other approaches."

c. Establish a connection to a medical record with biologic certainty. When a healthcare professional creates a record as part of an in-person encounter, the right biometric authenticator can memorialize that connection for the life of the patient, regardless of whether all the demographic data elements are determined. This is particularly useful in the care of indigent patients, who are often homeless and transient.

d. Can support life-saving emergency decision making. If a patient is unable to communicate, the right biometric can affirm connection to the trust anchor and make the patient's identity and relevant records known.

4. *Federate patient identity, so that a patient may be authenticated wherever (s)he appears in the continuum of care*. Value-based care requires close coordination between healthcare professionals across a distributed and often unaffiliated care continuum (as is the case in some forms of Accountable Care Organizations). As discussed above, **the foundation for achieving this level of interoperability is certainty about a patient's identity**. Federating patient identity makes the trust anchor available to authorized subscribers in a defined care continuum (e.g. TEFCA QHINs, their Participants, and Participant Members).

5. *Perform proactive lifecycle management of established patient identities. Demographic data elements change*. Unique identifiers may be added (e.g. a patient ages into Medicare, a national identifier is established). Additional historical records may be discovered. Duplicate or overlaid records may be discovered and resolved via referential matching technology. Unforeseen care in a new location (e.g. emergency care, urgent care) may occur, generating a new record and associated MRN. **The use of appropriate authenticators maintains the trust anchor and provides a secure location to add or update relevant demographic data elements, unique identifiers, and other attributes over the lifetime of a patient**.

As cited in a 2018 research report by The Pew Charitable Trusts, biometric authenticators and referential matching are two of four cornerstone opportunities to improve patient matching in the exchange of health information. By deploying those technologies in a 5-step process of robust identity proofing to establish a trust anchor, searching for historical records informed by the trust anchor, issuing appropriate authenticators at enrollment, federating identity, and proactively managing the lifecycle of patient identities, healthcare organizations can accurately and consistently match patients to their medical records. This solution will help providers, who are preparing to provide accurate patient information consistent with forthcoming regulations by ONC and CMS, support patient-directed access, and eliminate "information blocking." Additionally, there is a need for accurate patient data to feed new initiatives like analytics, telemedicine, precision medicine, social determinants of health, and clinical decision support.

According to Black Book Research, an average of 18 percent of a health system's records are duplicates, meaning almost one in five patients do not have a complete medical record present when important decisions are made at the point of care. Healthcare organizations must deploy robust patient identity methods to eliminate these duplicate records, assemble complete care histories, reduce redundant tests and procedures, and enable their patient engagement, patient access, and patient safety agendas.

We are impressed by the courage of ONC in taking on the challenge of achieving interoperability. We encourage you to continue aggressively and thoughtfully. Should you have any questions around the comments above, please contact Kerry Pillion via email at kpillion@imprivata.com or phone at (781) 761-1452.

Best regards,

Gus Malezis

President & CEO, Imprivata