U.S. Department of Health and Human Services
Office of the National Coordinator for Health IT
200 Independence Avenue, S.W.
Washington, D.C. 20201
ATTN: Steven Posnack and Kathryn Marchesini, Office of the Assistant Secretary for Technology Policy

Re: Individual Access Services on TEFCA and Wrong Record Scenarios

Unlike HIPAA or the FTC Health Breach Notification Rule, TEFCA imposes reporting obligations on recipients of TEFCA Information. These reporting obligations will promote discovery of Security Incidents or Threat Conditions by disclosing entities so they can determine their breach reporting obligations under applicable law (in most cases, the HIPAA Breach Notification Rule. The SOP's reporting requirements add another transparency pillar to promote trust in TEFCA, which is good.

However, the SOP falls short by 1) recognizing a breach exception for covered entity to covered entity disclosures that does not exist in HIPAA, 2) not incorporating the "low probability of compromise" analysis that is an essential part of the HIPAA Breach Notification Rule, and 3) not expressly incorporating the HITECH breach notification rules for personal health records, which cover non-HIPAA IAS providers.

Any unauthorized disclosure by a HIPAA Covered Entity to an unrelated entity, even a HIPAA entity, is considered a breach under HIPAA. **There is no statutory or regulatory exception to the definition of "breach" for disclosures outside of an entity covered by HIPAA.** The exceptions to the definition of "breach" in HIPAA are as follows:

- Unintentional "acquisition, access, or use" of PHI by an authorized person at a covered entity or business associate, if done in good faith and within the scope of authority, and there is no further use or disclosure in a manner not permitted by HIPAA. (45 CFR 164.402(1)(i).) Disclosures to another covered entity are part of the TEFCA SOP exception - but they are not part of the exception under HIPAA. The preamble to the final Breach Notification Rule provides an example of a billing employee within a covered entity receiving an e-mail sent by a nurse at the same covered entity that was not intended for the billing employee. (74 Fed. Reg. 42740, at 42747 (Aug. 24, 2009).). The preamble does not offer any other examples to suggest that the exception applies to the acquisition, access or use of another covered entity's patient record by an authorized person at an unrelated covered entity.

- Any "inadvertent disclosure" by an authorized person at a covered entity or business associate to another person authorized to access PHI "at the same covered entity or business associate (or organized health care arrangement which the covered entity participates), and the information is not further used or disclosed in a manner not permitted by HIPAA. (45 CFR 164.402(1)(ii).) The

preamble explains "this exception encompasses circumstances in which a person who is authorized to use or disclose protected health information within a covered entity, business associate, or organized health care arrangement inadvertently discloses that information to another person who is authorized to use or disclose protected health information within the same covered entity, business associate, or organized health care arrangement, as long as the recipient does not further use or disclose the information in violation of the Privacy Rule." (74 Fed. Reg. at 42748 (emphasis added); we presume OCR is expressly recognizing that in some cases, access within an entity - for example, by a member of the medical staff within a hospital - is considered to be a disclosure.)

- A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (45 CFR 164.402(1)(iii).) The preamble provides the following example: "a nurse mistakenly hands a patient the discharge papers belonging to another patient, but she quickly realizes her mistake and recovers the protected health information from the patient." (74 Fed. Reg. at 42748.)

None of the limited exclusions from the Breach definition apply when covered entities (or business associates working on their behalf) disclose PHI to another covered entity (or that covered entity's business associate). That means for covered entities and business associates, unauthorized disclosures upon discovery are presumptively considered to be reportable breaches under HIPAA unless the disclosing entity, after conducting and documenting the results of a low probability of compromise analysis,, concludes that the Breach is not reportable. The preamble supports this interpretation:

> If, for example, protected health information is impermissibly disclosed to another entity governed by the HIPAA Privacy and Security Rules or to a Federal agency that is obligated to comply with the Privacy Act of 1974 (5 U.S.C. 552a) and the Federal Information Security Management Act of 2002 (44 U.S.C. 3541 et seq.), there **may be less** [emphasis added] risk of harm to the individual, since the recipient entity is obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information. In contrast, if protected health information is impermissibly disclosed to any entity or person that does not have similar obligations to maintain the privacy and security of the information, the risk of harm to the individual is much greater. (74 Fed. Reg. 42740, at 42744 (Aug. 24, 2009).)

By endorsing a breach "exception" where none exists in the law, TEFCA is opening the floodgates to countless numbers of breaches and at least suggesting those are not reportable to patients or regulators. This mismatch between the SOP and the law could have significant negative impacts on patient privacy and efforts to build trust stewardship in TEFCA. The new TEFCA documents anticipate that records for 100s of potential matches might be shared to facilitate exchange, at least among disparate covered entities. If the SOP does not impose reporting obligations on all recipients of mismatched records to the disclosing organizations, there will not be any accountability for the way these mismatched records are accessed, used or re-disclosed downstream.

The SOP should instead follow HIPAA's Breach Notification Rules for the exceptions for breaches, and expressly call for a low probability of compromise analysis to be conducted by the disclosing entity after receiving notification of any mismatched record. HIPAA requires this analysis to be performed regardless of whether the third -party recipient of the wrong record is or isn't a HIPAA entity. Equalizing treatment of breaches for all purposes of use will also enable the REC to assure exchange for all of its priority use cases – and not just for treatment. Also, TEFCA's conditions of participation which require HIPAA compliance even of entities not technically covered by HIPAA adds further credence to an approach that treats all potential breaches as requiring the same principled approach. The REC has worked diligently to create a trust environment that supports a broad array of legally permissible use cases; it should continue to apply that approach with respect to all of its SOPs.

It is also important to note that this SOP as currently drafted, however well intended, undermines efforts to facilitate individual access through TEFCA. One of the reasons Individual Access Services is blocked from meaningful adoption on networks is that disclosing entities believe that sending the wrong record to a non-HIPAA IAS provider is automatically a breach under HIPAA, triggering potential notification requirements – **and they wrongfully believe this breach liability categorically does not exist when they disclose the wrong record to another covered entity.**

But as pointed out above, this is not the case under the law. Instead, disclosures of PHI by HIPAA covered entities are always presumptively breaches, regardless of who is the recipient. A low probability of compromise analysis is always going to be required by HIPAA for wrong record disclosures, and the SOP should reflect this.

Moreover, and as noted above, in the preamble to the final Breach Notification Rule preamble, OCR already opened the door to the possibility of a low probability of compromise determination when PHI is disclosed to another covered entity that is "obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information." Because all data "partners" participating in TEFCA are required to comply with HIPAA privacy and security rules under the flow-down provisions of the Common Agreement, there is ample opportunity for disclosing entities to consider those framework protections when determining what the risk is of a wrong record being sent to another TEFCA participant or subparticipant. Stated differently, IAS Providers are obligated under TEFCA to adhere to many standards and implementation requirements from the HIPAA Rules; when they do so, and also report a mismatched record and prevent re-use or re-disclosure, they reinforce TEFCA trust principles and support an ability for disclosing entities to conduct the low probability of analysis for presumptive breaches, the same way they would for other unauthorized disclosures.

This is particularly the case when a mismatched record is returned or securely destroyed and not further exposed to the wrong patient. In the breach rule preamble, OCR further stated "[w]e expect that there may be circumstances where a covered entity takes immediate steps to mitigate an impermissible use or disclosure, such as *by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed.* If such steps eliminate or reduce the risk of harm to the individual to a less than ''significant risk,'' then we interpret that the security and privacy of the information has not been compromised and, therefore, no breach has occurred." (74 Fed. Reg. at 42744-42745 (emphasis added).)

The SOP already requires recipients to notify disclosing entities of wrong record receipts. Further, personal health records under HITECH (which is all IAS Providers not covered by HIPAA) are already obligated under the FTC's Health Data Breach Notification Rule to notify individuals and the FTC if they breach an individual's health information, which would be the case if that IAS Provider accepted a patient's record received through TEFCA and populated it into the wrong patient account. The security incident/data breach SOP should be modified to expressly incorporate this important safeguard of patient rights and how it impacts the receipt of wrong records by IAS providers not covered by HIPAA under this SOP.

In conclusion, we make the following requests for updates to the SOP:

1. Consider all disclosures of wrong records as reportable TEFCA Security Incidents
2. Affirmatively require HIPAA Entities in receipt of a TEFCA Security Incident Notice to perform a low probability of compromise analysis, consistent with their obligations in the HIPAA breach notification rule
3. Affirmatively require non-HIPAA Entities to adhere to the FTC Health Breach Notification Rule whenever it either receives unencrypted Individually Identifiable Information for a person that has not accepted their Terms and Conditions, including their Privacy Notice, or populates a patient account with records for the wrong person.
4. Make an explicit policy statement that any recipient of wrong records not use or retain a record that is not in your census already