Summary of Recommendations

- **Accelerated Compliance Deadlines:** Recommend moving the compliance date for Approach 2 to August 1, 2026, instead of the proposed later deadlines. It suggests starting with a stricter matching algorithm and introducing softer matching after gaining more operational experience.
- **Define this as a roadmap**: 3+4 Matching is a great starting point, but we should improve methods and processes as we build to universal interoperability between all stakeholders (including individuals) while maintaining the high security and privacy setpoint that is appropriate and expected of individual's protected health information.
- **Optionality for Self-Asserted Data Sharing:** It is advised to change the requirement for sharing self-asserted demographic information from "SHALL" to "MAY," citing HIPAA's minimum necessary standard and the importance of patient choice in data sharing.
- **Patient Matching Responsibility:** The responsibility for patient demographic double-checking should rest with QHINs rather than IAS Providers, due to QHINs' experience and regulatory requirements. Consistent and comprehensive Record Locator Service (RLS) logic at the QHIN level is encouraged to improve matching accuracy.
- **Maintaining Error Notification Requirements:** The requirement for IAS Providers to notify relevant parties and purge data when a patient reports receiving another individual's data is supported, as it helps identify and correct errors.
- **Consent for IAS Use:** Recommend removing the specification for express documented consent for IAS use, stating that patients are not third parties to their own data and that IASPs act as vehicles for patient-directed access.
- **IASP Obligations Over Digital Assertions:** Trust in TEFCA should be built through clear policy, controls, and audits rather than new digital consent assertions, which are seen as unnecessary and complicating rollout.
- **Consistency in Matching Rules:** Recommend removing variability in matching rules for Responding Nodes, prioritizing a simple, consistent approach for trust, operational ease, and effective troubleshooting.

- **Consumer Choice in Identity Token Data Elements:** It is suggested that certain sensitive data elements (e.g., SSN) only be included in identity tokens if consented to by consumers, addressing privacy concerns and the principle of minimal necessary information.

4.3 Compliance Deadlines

We acknowledge the roadmap for compelled response in Section 4.8; however, we believe the Approach 2 deadlines should be accelerated. Because matching validated demographics has long been required for IAS, extending compliance to mid-to-late 2027 undermines trust in TEFCA's goals. We recommend moving the deadline to August 1, 2026.

To reduce variability in matching logic, we also suggest eliminating required use of self-asserted demographics and name synonyms. Instead, TEFCA should implement a stricter algorithm first and add softer matching later as experience with IAS grows across the framework. It is in fact a higher matching bar than what has been discussed in other forums such as the CMS Interoperability patient matching discussion. The CMS workgroup has taken the approach of using defined permutations (26 currently) two of which are:

First Name + Last Name + DOB + Phone Number

First Name + Last Name + DOB + Email Address

The proposed 3+4 logic is a high bar—higher than approaches discussed in other forums, including the CMS Interoperability patient matching discussion. In that CMS workgroup, defined permutations such as the two examples above suggest that phone number or email can function as a strong additional identifier (i.e., a low likelihood of false positives). In practice, that is closer to a 3+1 model than 3+4.

We recognize that email and phone can be "super matchers" and believe that the CMS matching workgroup and others are on a positive path to simplifying matching. However, the availability of some demographic across current interoperability connections is inconsistent; name, DOB, and address are widely present, while email and phone often are not.

If the choice is between (1) additional statistical analysis to further validate the CMS workgroup's conclusions (and/or parallel efforts) and (2) implementing an admittedly stringent 3+4 algorithm within months at scale, we favor implementing 3+4 now and iterating based on evidence. Once compelled responses using 3+4 are in place, we can audit cleared matches and test assumptions (e.g., "Record X matched Record Y—what

happens if we remove demographics A and B? Do we introduce collisions or still maintain accurate matches?"). Where no privacy collision occurs, those elements may be unnecessary and could be removed or re-weighted to make matching easier, safer, and broader. The key is to start.

4.5.g. IAS Queries initiated by an IAS Provider MUST also include all self-asserted demographic information not verified by the CSP that the IAS Provider may have collected from the Individual for the purposes of matching demographics.

It is recommended to change "SHALL" to "MAY." The rationale is that patients and consumers have the right to restrict how much data they share with third parties. In addition, HIPAA standards like the minimum necessary principle should be followed. Until there is a clear understanding of how collectively self-asserted data will be used, it is best not to share these values in order to meet the minimal necessary requirements.

4.6.a) When an IAS Provider receives a successful patient discovery response from a Responding Node, the IAS Provider MUST perform a patient demographics match comparison using its own algorithm with both IAL2 verified and self-asserted data in the IAS Provider's system against the demographics returned in the patient discovery response from the Responding Node ("Demographics Double-Check").

Change the double check requirement so it applies to QHINs instead of IASPs.

Reasoning: Placing this responsibility with QHINs improves control over inappropriate data sharing by addressing issues earlier. QHINs possess experience in patient matching, adhere to TEFCA controls, and often operate as BAAs, whereas IASPs are not direct QTF participants, do not undergo strict qualification processes, nor require advanced certifications like HITRUST R2 with HIPAA controls. Additionally, most current QHINs act as BAAs for covered entities or their agents.

The QTF allows QHINs to delegate patient matching when their RLS doesn't leverage an MPI. Ideally, all QHINs would support complete RLS functionality without passing matching requests downstream, preserving performance and consistency. Where this isn't feasible,

QHINs should still coordinate double-checks at their level with Participating or Subparticipants.

With compelled responses for IAS approaching, we recommend reviewing RLS features, as comprehensive patient search results between QHINs remain uncertain. For example, a non-comprehensive search or failed matches across federated entities can lead to "no patient found" errors, even when relevant data exists.

When a requestor gets the response "no patient matches found" from QHIN X, it is unclear if QHIN X attempted to be comprehensive or not in its data search. For a QHIN that federates patient matching to its data holding entities and has 2000 of them, all the following could yield *no patient found* even though five entities that are members of the QHIN have data for the patient.

- QHIN X fans in the patient discovery request to all 2000. All individual nodes timeout responding to QHIN X and QHIN X responds to the requestor with no patient found. The requestor would have no knowledge of the timeouts and would only receive the response *No patients found*.
- QHIN X geolocates to all entities in its QHIN within ten miles of the patient's address. This geoboundary yielded five practices but none had this particular patient.
- QHIN X fans in the request to all 2000. All respond in time with no patient found. The five sites with data have MPIs that were unable to match to the patient's provided demographics.

These issues will become more visible to patients who expect their records to be accessible through TEFCA, and operational gaps will be harder to explain or diagnose without consistent RLS logic.

4.6.b) If after viewing the TEFCA Information returned via an IAS Query by an IAS Provider, an Individual notifies the IAS Provider that they believe another Individual's data has been attributed to them, the IAS Provider MUST:

> *i. Notify the QHIN, Participant, or Subparticipant associated with the Responding Node that its customer has affirmatively indicated that they have received the wrong person's data. In this scenario, unless the QHIN, Participant, or Subparticipant identifies other breach mitigation factors, it would likely need to follow the HIPAA Breach Notification Rule's requirements for a one-person breach; and*

ii. Have a process in place to purge the erroneous data.

Recommend maintaining this requirement. Double checking on the matched demographics is a good control, but other errors do occur (example: errant patient record merges) which can expose the wrong data to patients. This would enable patients to assist in the finding and correction of errors.

As a related comment, we are not opposed to a "triple-check" standard for demographic matching—especially if it helps the framework move to a compelled-response position sooner. Under this approach: (1) the responding endpoint performs the initial match; (2) the requesting QHIN independently verifies the match before passing patient identifiers to the IASP; and (3) the IASP performs its own check as well. Requiring the requesting QHIN (servicing the IASP) to double-check adds an additional security and privacy control, helping prevent disclosure by responding data sources beyond their HIPAA boundary. This is a team sport.

4.8.a): From August 1, 2026 to July 31, 2027, Response Approach 2a or Respond Approach 2b below is optional for Responding Nodes with FHIR Endpoints published in the RCE Directory Service. As of August 1, 2027, all Responding Nodes MUST Respond in accordance with Response Approach 2a or Response Approach 2b. Responding Nodes with a FHIR Endpoint MUST also continue to Respond in accordance with Approach 1.

Reference introductory comments on Section 4.3. We maintain the timelines seem unnecessary long.

4.8.d)i. The IAS Provider has provided the express documented and informed consent(s) ("TEFCA IAS Consent") that validates and verifies that the individual has consented to use the Individual Access Service

Recommendation: Removal

Rationale: "Consent" appears inappropriate in this context because a patient requesting their own data is not a third party. We understand the RCE/ONC may have received input

that treats IASPs as third parties rather than patient-directed intermediaries. If so, we believe that interpretation is incorrect: the IASP facilitates the exchange, but the patient remains the recipient.

IAL2 is a NIST identity assurance level for digital transactions. Achieving IAL2 provides a high degree of confidence that the individual is who they claim to be. When an individual is verified at IAL2, the transaction can be treated as originating from that individual, and any stated exchange preferences can be treated as their directives.

In addition, we support adoption of an IASP code of conduct to promote transparency in data use, clarify individuals' rights to authorize downstream exchanges, and enable data deletion or content purging when desired. These measures reinforce that the individual is the primary recipient and that IASPs must act in accordance with the individual's directives.

Data holders can continue to document the time, date, and content of exchanges without adding separate consent transactions. Because the transaction is already patient-directed, additional "assertion" protocols would be duplicative and would likely require specifications beyond what TEFCA SOPs currently describe. That added complexity could delay IAS implementation and could imply—incorrectly—that IAS is not a direct, patient-directed transaction for access to the patient's own data. Such delays are unnecessary and inconsistent with federal requirements protecting patient access rights.

4.8.1 TEFCA IAS Consent Policy

Consistent with the above, we believe this should switch to obligations of the IASP and not digital assertions. TEFCA has the opportunity to create trust and can do so through policy, controls, and audits of the technology and actions of IASPs and QHINs. Adding new digital assertions to the already stringent standards for IAS seems substantively unnecessary.

4.8.2 Matching Rules for Responding Nodes

Subsection b): Recommendation for Removal.

Reasoning: Although this variability can be helpful in certain exchanges, it ultimately complicates the enforcement of mandatory IAS responses by slowing down processes.

Firstly, there are known situations that result in false positives, such as twins with similar names living at the same address. While solutions exist, they tend to be more complex

than the straightforward "3 + 4" method outlined in the SOP. Prioritizing practicality, we suggest moving quickly to a unified, simple matching system and addressing more intricate issues like false negatives at a later stage.

Secondly, maintaining consistency enhances trust, operational efficiency, and troubleshooting. Rather than permitting name variations, it's more effective to educate consumers and patients about their clinical records and the need for consistent demographic information. At present, accessing clinical data is difficult for consumers. Once scalable infrastructure is established through TEFCA and compulsory T-IAS responses from data holders, efforts can shift to resolving remaining challenges. For example, if I use an IASP and receive results from seven out of eight practices, all listed on TEFCA, I know to contact the eighth practice to update my demographics and enable data sharing. Educating consumers about medical record accuracy, data security, and ways to use their information to improve health should include explaining the importance of providing official names, addresses, and related details.

4.8 Response Requirement Approaches

We recommend reversing the order of Approaches 2a/2b, making them the Nominal Flow, with Approach 1 as the Alternate Flow. Labeling something as "1" suggests it is the primary option, but Approach 1 was added later and it's the language in the SOP caused confusion. Clarity on intent is best served by ordering this properly and making 100% clear that the nominal flow MUST be supported and the Alternate may be supported but SHALL NOT be used to be substitute for the primary. Optionality is detrimental to the rollout of data and process standards and we must be clear, without room for misinterpretation, or we will continue to have noncompliance and/or misaligned results compared to expectations.

4.9 Identity Token Requirements

Table 2: Create a category for MUST be included if consented to by the consumer.

Reasoning: We have heard concern about the forced sharing of some data elements from the CSP to the IASP. Some data, such as SSN, is considered sensitive by consumers and healthcare alike. Given matching does not require all to be included to function, we should consider allowing some variation in what the CSP "knows" and what it is required to share with IASP.