Draft: Exchange Purpose (XP) Implementation SOP: Individual Access Services (IAS)

Version 3.0

Deleted: 2.1

Effective Date:

Deleted: April 11, 2025

Applicability:

4.1 - 4.4, 4.6, 4.8 – 4.9: IAS Providers

Deleted: 6

4.5, 4.8 – 4.9: QHINs, Participants, Subparticipants

Deleted: .7, 4

1 Common Agreement References

The requirements set forth in this Standard Operating Procedure (SOP) are for implementation, in addition to the terms and conditions found in the Framework Agreements, the Qualified Health Information Network® (QHIN™) Technical Framework (QTF), and applicable SOPs. The Trusted Exchange Framework and Common Agreement™ (TEFCA™) Cross Reference Resource identifies which SOPs provide additional detail on specific references from the Common Agreement.

All documents cited in this SOP can be found on the Recognized Coordinating Entity® (RCE®) website.

2 SOP Definitions

Select terms used throughout this SOP are defined in this Section for ease of reference. All capitalized terms used in this SOP have the respective meanings assigned to such term in the TEFCA Glossary.

Individual Access Services (IAS): the services provided to an Individual by a QHIN, Participant, or Subparticipant that has a direct contractual relationship with such Individual in which the QHIN, Participant, or Subparticipant, as applicable, agrees to satisfy that Individual's ability to use TEFCA Exchange to access, inspect, obtain, or transmit a copy of that Individual's Required Information.

Individual Access Services Provider (IAS Provider): each QHIN, Participant, and Subparticipant that offers Individual Access Services (IAS).

TEFCA IAS FHIR Endpoint: The FHIR Endpoint that is listed in the RCE Directory Service and Responds to IAS Queries.

Deleted: Terms defined in this Section are introduced here and can be found in the TEFCA Glossary. Capitalized terms used in this SOP have the respective meanings assigned to such term in the TEFCA Glossary. ¶
No new definitions are introduced in this SOP.¶
The following defined terms from the Common Agreement and other SOPs are repeated here for reference.¶

3 Purpose

This SOP identifies specific requirements that IAS Providers are required to follow for Individual identity verification when sending an IAS Query. This SOP also identifies when a QHIN, Participant, or Subparticipant is required to Respond to an IAS Query.[1] This SOP includes context-specific privacy and security transaction requirements for IAS Providers. Privacy and security requirements for IAS Providers are included in the IAS Provider Requirements SOP, along with the Common Agreement.

Deleted: out of scope for this SOP and are

[1] Nothing in this SOP alters a Covered Entity's obligations under applicable law.

Deleted: the HIPAA Rules

4 INDIVIDUAL ACCESS SERVICES (T-IAS)

4.1. Exchange Purpose Code (XP Code)

a) All TEFCA Exchange under IAS MUST use the XP Code T-IAS.

4.2. QHIN Technical Framework (QTF)

a) All TEFCA Exchange under IAS MUST follow technical requirements as specified in the QTF.

b) If QHINs, Participants or Subparticipants are using Facilitated FHIR-based flows in support of their IAS exchange, the TEFCA Exchange MUST also follow the technical requirements as specified in the Facilitated FHIR Implementation SOP.

4.3. IAS Provider Use of Approved Credential Service Providers (CSPs)

IAS Providers are only permitted to use CSPs that have been approved by an RCE-selected CSP approval organization. IAS Providers MUST ensure the CSP(s) it partners with do the following:

a) Conduct identity proofing to at least Identity Assurance Level 2 (NIST IAL2) as defined by the then latest version of NIST SP800-63A.

b) Be able to verify the following demographic information[2]:

i. First Name
ii. Middle Name/Middle Initial
iii. Last Name
iv. Suffix
v. Date of Birth
vi. Street Address
vii. City
viii. State
ix. Zip Code
x. Email
xi. Mobile Phone #
xii. State ID/Drivers License #
xiii. SSN Last Four

c) After verifying an Individual's identity, deliver to the IAS Provider a signed (with the CSP's private key) IAL2 Claims Token in the OpenID Connect format (as detailed in Section 4.9)

[2] IAS Providers are encouraged to look for CSPs that can verify historical addresses, additional email addresses, additional mobile phone numbers, and provide a CSP Issued Identifier (if issued as a customer digital identifier).

Deleted: and the Facilitated FHIR Implementation SOP

Formatted: Not Highlight

Deleted: Definition¶
TEFCA Exchange under the XP Code T-IAS means the services provided to an Individual by a QHIN, Participant, or Subparticipant that has a direct contractual relationship with such Individual in which the QHIN, Participant, or Subparticipant, as applicable, agrees to satisfy that Individual's ability to use TEFCA Exchange to access, inspect, obtain, or transmit a copy of that Individual's Required Information.¶

Formatted: Not Highlight

Deleted: <#>IAS Providers MUST have an agreement with a credential service provider (CSP) that has been approved by an RCE-selected CSP approval organization.[3] ¶
The CSP approval organization must maintain a published list of CSPs who conduct identity proofing to at least Identity Assurance Level 2 (NIST IAL2) as defined by the then latest version of NIST SP800-63A. The CSP approval organization MUST require approved CSPs to be assessed for conformance to the minimum appropriate identity proofing and credential management standards, and to publish and maintain the standards to which the CSPs are assessed. ¶

Deleted: <#>on behalf of

Deleted: <#>, the CSP MUST make available to that IAS Provider a signed …

Deleted: <#>token

with the Individual's demographics that were verified by the CSP, including the CSP Public Subject Identifier.[4]

d) Provide a publicly accessible endpoint (without authentication) to share a JSON Web Key Set (JWKS), which Initiating Nodes and Responding Nodes are able to use to validate an identity token issued by that CSP. The private key used to create the signed token has a corresponding public key found in the JWKS document mentioned above, whose URL is found in the jwks_uri metadata value provided by the CSP.[5]

e) Supply configuration information per *OpenID Connect Discovery 1.0 incorporating errata set 2: Obtaining OpenID Provider Configuration Information*. Configuration values are known as OpenID Provider Metadata. From the OpenID specification: OpenID Providers supporting Discovery MUST make a JSON document available at the path formed by concatenating the string /.well-known/openid-configuration to the Issuer.

4.4. IAS Provider Responsibilities

a) IAS Providers MUST have an agreement with a CSP that has been approved by an RCE-selected CSP approval organization.[8]

b) IAS Providers MUST authenticate Individuals using processes set to at least Authenticator Assurance Level 2[9] (AAL2) requirements.

c) IAS Providers MUST ensure the identities of Individuals that elect to use their IAS offering are verified to at least NIST IAL2 via a CSP when any of the following occurs:

i. Prior to the Individual's first use of TEFCA Exchange,

ii. When verified demographics change, or

iii. When the verified demographics expire or are otherwise invalidated by the CSP.

d) An IAS Provider MUST include the following IAL2-verified demographics in an IAS Query for the Query to be valid and usable for TEFCA Exchange:

i. First Name
ii. Last Name
iii. Date of Birth
iv. Street Address
v. City
vi. State
vii. Zip Code, and
viii. *Either* email address *or* mobile phone

[4] In the OpenID Connect Protocol, the CSP implements the requirements of the OpenID Provider.

[5] CSP are encouraged to rotate encryption keys as described in OpenID Connect Core. See Final: OpenID Connect Core 1.0 incorporating errata set 2 for details.

[8] The RCE-selected CSP approval organizations are published and maintained on the RCE website.

[9] See https://pages.nist.gov/800-63-3-Implementation-Resources/63B/AAL/ for full information on the levels.

Deleted: <#>. Each CSP will p

Deleted: n

Deleted: a

Deleted: MAY

Deleted: <#>The CSP signs the token with a private key and publishes the corresponding public key at <iss>/.well-known/openid-configuration per OpenID Connect Discovery[6]. For example, if the ID token's iss element is https://csp.example.com, the CSP's JWKS document would be available at: https://csp.example.com/.well-known/openid-configuration. The CSP MUST provide the JWKS publicly without requiring authentication. CSP are encouraged to rotate encryption keys as described in OpenID Connect Core[7]¶
Initiating Nodes and Responding nodes MAY use the public key to verify the CSP's signature on demographics included in the JSON Web Token (JWT.) ¶

Deleted: <#>**Individual Verification**

Deleted: verify

Deleted: p

Deleted: w

Deleted: and

Deleted: after credentials expire. An IAS Provider MUST ensure that all updates to demographic information used for TEFCA Exchange for IAS are validated to NIST IAL2 by the CSP prior to their use.¶

Deleted: s

Deleted: q

Deleted: demonstrate that all Individuals that elect to use their IAS offering have proven their identities consistent with achieving NIST IAL2. This evidence MUST be included within the Query as an IAL2 Claims Token using the OpenID Connect token format as detailed in Section 4.6.

Deleted: levels

e) An IAS Provider MUST include all the IAL2-verified demographics provided by its CSP in the IAS Query even when more than the minimum needed for a valid IAS Query have been verified.

f) IAS Queries initiated by an IAS Provider MUST contain the IAL2 Claims Token.

4.5. Required Information

a) Required Information is specified in the Exchange Purposes (XPs) SOP.

4.6. Response Requirement Approaches

Upon receipt of a valid IAS Query, Responding Nodes MUST support at least one of the following modes for Individuals to access Required Information[11]:

a) **Response Mode 1 – Individual Authentication-based**

1.1. When a Responding Node with a TEFCA IAS FHIR Endpoint achieves a possible match[12], it MUST Respond with the applicable TEFCA IAS FHIR Endpoint for the Individual to access their Required Information via Responder-supported authentication mechanisms (e.g., password, passkey).

1.2. On and after [DATE], all TEFCA IAS FHIR Endpoints deployed for Response Mode 1 MUST support the requirements in the HL7 SSRAA FHIR IG as outlined in the Facilitated FHIR Implementation SOP.

b) **Response Mode 2 – Verified Identity-based**

2.1. When a Responding Node achieves an acceptable, uniquely attributable demographics-based match for an Individual according to its matching policy[14], it MUST Respond to the Patient Discovery Query and MUST provide at least one of the following without requiring the Individual to separately log-in to the Responding Node:

[11] All Q/P/S that have a Node that is required in regulation to support individual access APIs are recommended to list the TEFCA IAS FHIR Endpoint for such Node in the RCE Directory Service to support Response Mode 1. This includes health care providers that have adopted Certified EHR Technology and deployed certified API technology (e.g., technology certified to 45 CFR 170.315(g)(10)), and health plans required by CMS rules.

[12] Because this mode is focused on returning individual authentication-based TEFCA IAS FHIR Endpoints, which will require subsequent action by an individual, the possibility of a match based on limited demographics (e.g., first name, last name, date of birth) should take priority to give Individuals the best chance of accessing their information from all locations on TEFCA.

[14] Responding Nodes should base their response policy on industry standard methods, accommodate high friction points like nickname resolution and address variation, and consider consensus-based approaches for patient matching such as those emerging from the CMS Health Tech Ecosystem.

Deleted: <#>For TEFCA Exchange under the XP Code T-IAS, beginning December 31, 2024, Required Information is, at least, the USCDI v1 data classes and data elements[10] that the Responding Node maintains. ¶
If the Responding Node is controlled by a Health Plan, the Responding Node MUST also share individual claims and encounter data (without provider remittances and enrollee cost-sharing information) that it maintains. ¶
Additional details on implementation specifications for Required Information are provided in the QTF and applicable XP Implementation SOP(s). For the avoidance of doubt, prior to January 1, 2026, the QTF does not require USCDI data to conform to USCDI vocabulary standards.¶

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Deleted: [13]

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Deleted: Individual Access

1) a patient identifier, which can be used to request documents with Required Information, or

2) a TEFCA IAS FHIR Endpoint, which can be used to authorize access to Required information.

2.2. When a Responder Responds using Response Mode 2, IAS Providers MUST perform the demographic-double check requirements as outlined in Section 4.7. If, following the IAS Provider's demographic-double check, the Responding Node receives a Document Query, the Responding Node MUST Respond with the Required Information per the Framework Agreements and Applicable Law.

2.3 On and after [DATE], all TEFCA IAS FHIR Endpoints deployed for Response Mode 2 MUST support the requirements in HL7 SSRAA FHIR IG as outlined in the Facilitated FHIR Implementation SOP.

4.7. IAS Provider Breach Mitigation Responsibilities

The following applies to an IAS Provider in the context of assisting HIPAA Covered Entities apply the four "low probability of compromise" factors established in paragraph (2) of the "breach" definition adopted at 45 CFR 164.402 of the HIPAA Breach Notification Rule. All other Applicable Laws continue to apply. IAS Provider breach reporting and notification responsibilities are set forth in the IAS Provider Requirements SOP.

a) When an IAS Provider receives a successful Patient Discovery Response from a Responding Node, via Response Mode 2 in Section 4.6, the IAS Provider MUST perform an Individual 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").

i. If the Demographics Double-Check does not determine a match between the IAL2 verified and self-asserted data in the IAS Provider's system and the demographics data returned by a Responding Node, the IAS Provider:

1) MUST reject the demographics response from the Responding Node, and

2) MUST NOT retain the patient identifier from the Individual's request, and

3) MUST NOT continue to initiate an IAS Query to that Responding Node and,

4) MAY provide the Individual with the Responding Node's Individual Authentication-based mode (Response Mode 1), if supported.

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Font: Not Highlight

Deleted: Any Responding Node that receives an IAS Query from an IAS Provider that includes the appropriate IAL2 Claims Token, as specified in 4.3(c), and that achieves an acceptable demographics-based match based on responder policy OR where responder issued credentials are presented MUST Respond with the Required Information per the Framework Agreements and Applicable Law.¶

Deleted: <#>Queries initiated by an IAS Provider MUST include only the demographics as provided to the CSP and as part of the Individual's identity verified to NIST IAL2. ¶

Formatted: Not Highlight

ii. When a Demographics Double-Check does not determine a match, preventing the use of Mode 2, the IAS Provider MUST notify the QHIN, Participant, or Subparticipant that operates or is associated with the Responding Node that returned the demographics. This can be done directly, or via the QHIN of the Responding Node.

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 all erroneous data.

4.8. Compliance Dates

Review the applicable SOP Section Numbers for more information regarding the requirements for these compliance dates.

SOP Section Number	Compliance Requirement	Applicability	Compliance Date
4.6	Modes 1.3 and 2.3: All TEFCA IAS FHIR Endpoints MUST support the requirements in HL7 SSRAA FHIR IG as outlined in the Facilitated FHIR Implementation SOP.	Q/P/S	[Date TBD]
4.7	Demographics Double Check	IAS Providers	[Date TBD]
4.9	IAL2 Claims Token requirements and SAML claim updates.	Q/P/S	[Date TBD]

4.9. Identity Token Requirements

a) The OpenID Connect Core [15] specification describes the OpenID Connect ID Token required for IAS Exchange. The following additional requirements apply:

[15] See http://openid.net/specs/openid-connect-core-1_0.html for details.

Formatted: Font: 12 pt, Not Highlight

Formatted: Font: (Default) Calibri, Font color: Black

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: No underline, Not Highlight

Deleted: <#>Verification of an Individual to at least NIST IAL2 MUST meet the following requirements: ¶
Verification MUST include, at a minimum, the following demographics: First Name, Last Name, Date of Birth, Address, City, State, and Zip Code. ¶
Verification SHOULD also include, but does not require the following demographics: Sex, Middle Name OR Middle Initial, Suffix, Email Address, Mobile Phone Number, Social Security Number (SSN) OR last four (4) digits of SSN, Zip Code+4, and other verifiable identifiers (e.g., Medical Record Number, Passport Number, Driver's License, or other Government Issued Identification).¶
Historical name and/or address information MAY be included only if validated by the CSP for identity proofing for that Individual.¶

Deleted: T-

Deleted: details

i. Public Keys Published as Bare JWKS: The CSP MUST publish public keys as bare JWKS, which MAY also be accompanied by X.509 representations of those keys.

ii. Signed ID Token: The CSP MUST support Signing ID Tokens with RSA SHA-256.

iii. Claims: The CSP MUST include the claims in Tables 1, 2 and 3, in addition to all other required OIDC Core claims. The CSP MUST NOT include unverified demographic claims in the token.

Deleted: below

Formatted: Not Highlight

Table 1: OpenID Connect (OIDC) JWT Header Claims

OIDC JWT Header	Description
alg	Hardcoded to "RS256".
kid	Identifies which key to use from the JWKS.
typ	Hardcoded to "JWT".

Deleted: ".

Table 2: OpenID Connect (OIDC) JWT Body Claims

OIDC JWT Body	Description
aud	HCID of the IAS Provider as a URI. For example, urn:oid:<oid> (per RFC 3061) MUST be used and MUST be the unique HCID of the IAS Provider's directory entry[16].
iat	When the CSP issued the token.
iss	The Issuer Identifier for the CSP. An HTTPS URL used as the base for OIDC Discovery. Validators retrieve JWKS key material via the `jwks_uri` value in `<iss>/.well-known/openid-configuration`.
jti	Unique identifier for the JWT.
csp_issued_identifier	The CSP Issued Identifier assigned to the individual. This differs from the OIDC claim 'sub', which is a required OIDC claim.
Demographics that MUST be included or use "Unknown" in your Query	
given_name	If the given name consists of multiple parts, they SHALL be delimited by space.
family_name	If the family name consists of multiple parts, they SHALL be delimited by space.

Deleted: 3001

Formatted: Not Highlight

Deleted: The base URL of the CSP at which the JWKS is accessible.

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Deleted: nickname ... [1]

[16] In standard OIDC, the `aud` claim contains the `client_id` assigned to the Relying Party by the OpenID Provider at the time of OAuth client registration. In TEFCA, the IAS Provider's HCID OID URI serves as the functional equivalent of the `client_id` for purposes of audience binding. CSPs MUST populate `aud` with the IAS Provider's HCID expressed as `urn:oid:<oid>` per RFC 3061, obtained from the TEFCA directory. IAS Providers MUST validate that the `aud` value in any received IAL2 Claims Token matches their own HCID OID URI. This substitution is a TEFCA-specific constraint on the OIDC `aud` claim and does not alter any other requirement of OIDC Core §2 or §3.1.3.7.

OIDC JWT Body	Description
birthdate	Represented in YYYY-MM-DD format according to ISO 8601-1. All three elements (year, month, and day) MUST be present; partial dates (with missing year or mm-dd) SHALL NOT be used.
address	Current verified address. A single JSON object per OIDC Core §5.1.1 and the additional requirements in Table 3.
email	Either verified email *or* verified phone number is required. Both can be included, but at least one of these MUST be present.
phone_number	
Demographics that MUST be included if known	
middle_name	
middle initial	
suffix	
ssn_last_four_digits	Extension
zip+4	Extension
Gender	

Formatted: Not Highlight

Deleted: See list and definition of address elements below. Allow multiple addresses (array) if supported by the CSP.

Deleted: historical_address ... [2]

Deleted: email ... [3]

Deleted: Last

Deleted: ZIP

Table 3: OpenID Connect (OIDC) JWT Body Address Objects

OIDC JWT Body Address Object	Note	Optionality
formatted	This field MAY contain multiple lines, separated by ("\r\n") or ("\n").	OPTIONAL
street_address		REQUIRED
locality	City of residence	REQUIRED
regionality	State of residence using the 2-letter codes defined in ISO 3166-2 for US states and territories.	REQUIRED
postal_code	ZIP Code	REQUIRED
country	Country code based on the 2-letter codes defined in ISO 3166-2.	REQUIRED

Deleted: , IF KNOWN

Deleted: , IF KNOWN

Deleted: , IF KNOWN

Deleted: , IF KNOWN

Deleted: , IF KNOWN

b) If known and verified, all additional claims (such as Historical Name) **MUST** be included by adding the claim labelled as:

`http://rce.sequoiaproject.org/OIDC/claim/[claim]`

Examples of the OIDC JWT are online at the RCE resources site here: <include URL in published version>

c) The OpenID Connect token MUST be included in all IAS Queries, including all Patient Discovery, Document Query, Document Retrieval, and FHIR Authentication.

d) An IAS Provider using QHIN Query MUST relay the CSP-provided OpenID Connect token[17] within its Query using an additional Security Assertion Markup Language (SAML) attribute with Name `urn:ietf:params:oauth:token-type:id_token` and NameFormat `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`, containing the OpenID Connect token in a QHIN Query or as an additional element ("id_token") within the TEFCA_IAS extension in the FHIR Query.

e) Examples are online at the RCE resources site here: <include URL in published version>

[17] See https://openid.net/specs/openid-connect-core-1_0.html#IDToken for details on base token requirements.

Deleted: <#>Additional Claims MAY be included as follows: Mother's Maiden Name, Birth Place Address, Birth Place Name, Principle Care Provider ID (i.e., NPI) by adding the claim labelled as http://rce.sequoiaproject.org/OIDC/claim/ [Claim] as indicated in the below example.¶
Example OIDC JWT¶
{¶
"alg":"RS256",¶
"kid":"toW9jMUSN/5/L3iwaQGdTmNDuhvp/JcAZVH/RGF2aWQgUHlrZQ==",¶
"typ":"JWT"¶
} ¶
{¶
"aud":"hci1",¶
"iat":1666280632,¶
"iss":"https://csp.example.com",¶
"sub":"f7bdf590-2fc4-4718-8f33-043c8f96b66d",¶
"jti":"bcb9533e-1cc1-48bd-848b-b4200ea504b9",¶
"given_name":"John",¶
"family_name":"Schmidt",¶
"middle_name":"Jacob Jingleheimer",¶
"nickname":"Ed",¶
"email":"jjjs@example.com",¶
"email_verified":true,¶
"phone_number":"555-555-5555",¶
"gender":"M",¶
"birthdate":"Unknown",¶
"address":{¶
→"formatted":"1060 West Addison Street, Chicago, IL 60613 USA",¶
→"street_address":"1060 West Addison Street",¶ ... [4]

Deleted: <#>the Security Assertion Markup Language (SAML)for

Deleted: <#>An IAS Provider using Facilitated FHIR MUST follow the requirements as set out in the Facilitated FHIR SOP.¶

Deleted: <#>statements

Deleted: <#>("id_token")

Deleted: <#>containing oasis:names:tc:SAML:2.0:cm:bearer

Deleted: <saml2:Attribute Name="id_token">¶
<saml2:Attribute NameFormat="oasis:names:tc:SAML:2.0:cm:bearer">¶
<saml2:AttributeValue>{Base64 encoded token}</saml2:AttributeValue>¶
</saml2:Attribute>

Deleted: **<#>Required Information**¶
For TEFCA Exchange under the XP Code T-IAS, beginning December 31, 2024, Required Information is, at least, the USCDI v1 data classes and data elements[18] that the Responding Node maintains. ¶
If the Responding Node is controlled by a Health Pl ... [5]

5 VERSION HISTORY

Version	Revision Date	Section #(s) of Update
1.0	September 16, 2022	First Release
2.0	August 6, 2024	All Sections
2.1	April 11, 2025	All Sections – Language aligned with Exchange Purposes (XPs) SOP Version 4.0
3.0	Xxx	All Sections

Page 8: [1] Deleted **Katie Crenshaw** **5/18/26 1:29:00 PM**

Page 9: [2] Deleted **Katie Crenshaw** **5/18/26 1:31:00 PM**

Page 9: [3] Deleted **Katie Crenshaw** **5/18/26 1:56:00 PM**

ssn_last_four_digits	Extension

Page 10: [4] Deleted **Katie Crenshaw** **5/18/26 1:58:00 PM**

Page 10: [5] Deleted **Katie Crenshaw** **5/18/26 1:08:00 PM**