(1) User authenticates him/herself to the local system, within the context of an authorized role.

(2) On behalf of authenticated and authorized user and role, local server sends metadata search parameters to DEAS.

(3) DEAS mediates request and searches metadata as permitted by privacy metadata within context of authorized role sent with query; transaction is recorded in audit trail.

(4) DEAS returns data locator list (e.g., URIs) resulting from metadata search.

(5) Local server requests data from URIs returned from DEAS.

(6) Data storage location server mediates request and returns encrypted records to local server.

(7) On behalf of authenticated and authorized user and role, server sends DEAS request for encryption key for each data element provided.

(8) DEAS mediates request, and retrieves key as authorized from key management service; transaction is recorded in audit trail.

(9) Local server decrypts data elements and makes available to user.

(10) After use, system destroys cleartext and key, possibly retaining ciphertext.

DEAS Security Mediation and Audit Services

Data Element Access Services (DEAS)

DEAS Metadata Search Service

DEAS Key Management Service

User's Local System

Data Storage Location

DEAS Services Bus

Metadata indexed and tagged in accordance with individual consumers' consents

Decryption keys stored apart from metadata and clinical data

Query mediation, transaction auditing, real-time audit analysis

Metadata indexed and tagged in accordance with individual consumers’ consents

Decryption keys stored apart from metadata and clinical data