

Recommendations on message handling in directed exchange:

We placed message handling into four basic categories [should provide examples in each category]:

- a. No intermediary involved (exchange is direct from point A to point B).
- b. Intermediary performs only routing and has no access to PHI (does not open message).
- c. Intermediary opens messages - has access to PHI - but does not change data.
- d. Intermediary opens message and changes the data.

We responded to these categories with the following recommendations:

- PHI exposure to an intermediary in any amount (whether in message content or in routing or metadata) raises privacy concerns.
- Best practices for directed exchange are found in models A and B above where no PHI is exposed. ONC should encourage the use of such models.
- Models c and d involve intermediary access to PHI. Clear policies are needed to limit intermediary retention of PHI and restrict its use and re-use. Our team may make further privacy policy recommendations concerning retention and reuse of data. Model d also should be required to make commitments regarding accuracy and quality of data transformation.
- Intermediaries using audit trails which include PHI should also be subject to such policy constraints.
- Business associate agreements may be one tool for enforcing such policies and commitments/representation.
- We also addressed the question of whether establishing exchange “credentials” should be centralized or decentralized (i.e., who holds the “trust”?)
- The responsibility for maintaining the privacy and security of a patient's

record rests with the patient's providers. For functions like issuing digital credentials or verifying provider identity, providers may delegate that authority to authorized organizations.

- To provide physicians and hospitals (and the public) with some reassurance that this credentialing responsibility is being delegated to a “trustworthy” organization, the federal government (ONC) has a role in establishing and enforcing clear requirements and policies about the credentialing process, which must include a requirement to validate the identity of the organization/individual requesting a credential.
- State governments can, at their option, also provide additional rules for these authorized credentialing organizations.