

What limits should be placed on the collection, use and disclosure of PHI by providers?

*Treatment/Coordination of Care:*

- Should disclosure of PHI through a HIE be limited to treatment of the subject individual? (Note: HHS has construed “treatment” to mean treatment of ANY patient not just the subject of the PHI. For example, a provider could look up the PHI of Patient A’s siblings to treat Patient A.)
- How, if at all, should it be determined that a treatment relationship exists between the provider and patient whose information is requested? Would trusting the requesting provider be sufficient? Attestation? What additional measures—such as security—might be desirable/needed?
- Will providers who are not covered by HIPAA be permitted to access PHI through a HIO? If so, what—if any—additional requirements should be placed on these providers?

*Public health reporting:*

- How should public health reporting be handled? As authorized by the record holder? Could the recordholder authorize electronic auto-disclosure if pursuant to lawful public health authority?

*Quality reporting:*

- How should quality reporting be handled? As authorized by the recordholder?

*Payment*

- To be addressed at a later date. Stage one meaningful use requires only insurance verification.

What limits should be placed on use, disclosure and retention of PHI by third-party service providers (aka "intermediaries") (include limits on HIO or database itself in those models?)

- Service must be to assist provider in fulfilling one of the purposes under Stage 1 of MU
- May use only information (identifiability and content) reasonably necessary to accomplish purpose?
- May not re-use for any other purpose (except as reasonably necessary to fulfill business function for which third-party has been hired) unless specifically requested to do so by record holder(s)? (including aggregation of data from multiple sources)
- May retain data only for as long as reasonably necessary to perform functions requested by the data holder (and activities reasonably related to those functions); retention policies must be established; at the end of retention period data must be securely returned or destroyed per NIST standards
- Transparency - third party service providers should disclose to their record holder customers how they use and disclose information, and their retention policies?
- Accountability - are business associate agreements sufficient?