

HcDir Tiger Teams



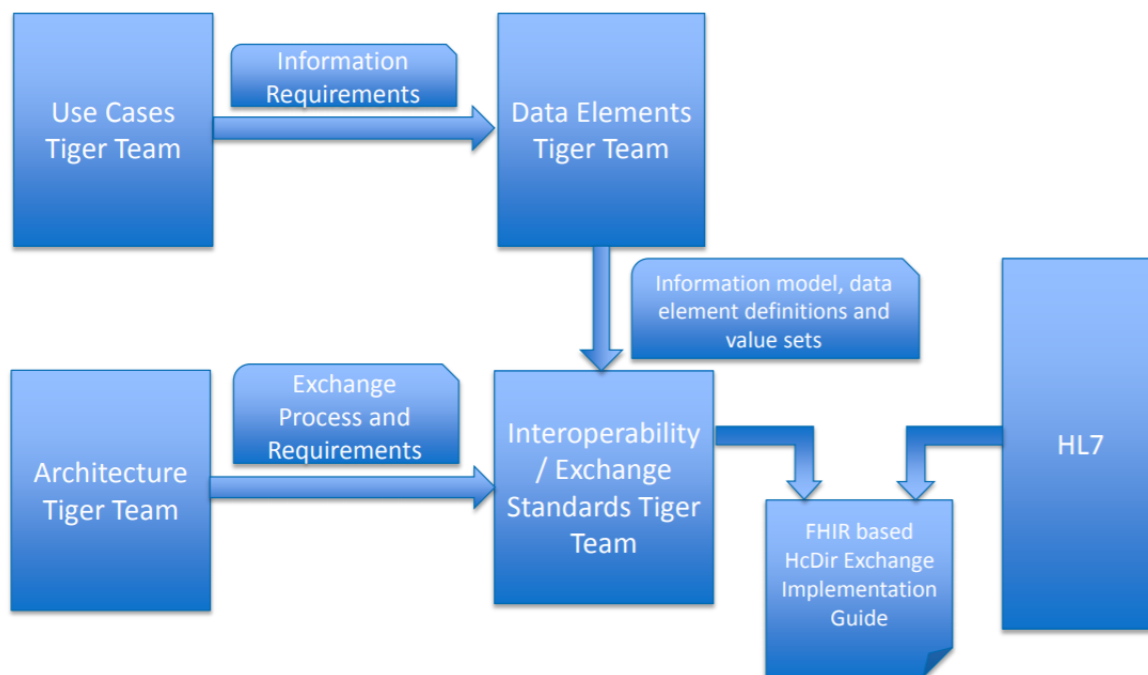
HcDir Tiger Teams

The ONC/FHA Healthcare Directory initiative established four Tiger Teams comprised of public and private sector stakeholders to guide this work. Tiger Team members were invited as subject matter experts and representatives of key stakeholder groups including:

- Providers
- Payers
- Health IT developers
- Health Information Exchange Organizations (HIEs/HIOs)
- Health Information Service Providers (HISPs)
- Professional & non-profit associations
- State government
- Federal government (ONC, FHA, SSA, CMS, DOD, VA)

Together, the Tiger Teams were charged with describing the Use Cases, Data Elements, Architecture, and Interoperability Standards associated with a proposed national resource of validated healthcare directory data

ONC-FHA Healthcare Directory Tiger Team Dependencies



Use Cases

The Tiger Team identified, developed, and tested a set of use cases supported by healthcare today. For each use case, the Tiger Team identified high-level information requirements to support the use case (e.g. demographics, location, electronic endpoint).

Data Elements

The Tiger Team defined all the data elements associated with the information requirements in the Use Cases Tiger Team, proposed value addition processes, and modeled the data in the Federal Health Information Model (FHIM). The Tiger Team evaluated existing standards (e.g. FHIR, IHE, S&I Framework) when defining the data

Interoperability

The interoperability tiger developed an HL7 FHIR-based implementation guide for the exchange of information between the national resource and local environments. The Tiger Team identified applicable FHIR resources, developed extensions, and proposed new resources.

Architecture

The Architecture Tiger Team defined a national architecture for the exchange of information between a national resource of validated healthcare directory data and local environments. The Tiger Team addressed issues such as mechanisms for exchanging information, capabilities for segmenting/constraining the data, and access controls, security, and encryption.