**Background**

Epic software enables Epic Community Members to monitor and manage applications' API access using application/client records and client IDs. When a developer registers an application, they create an application record which stores basic information about the application, including its developer, name, API scope, and auto-generated client IDs for production and non-production use.

The client IDs uniquely identify the application and associate it with the application record. The presence of client IDs in Subspace integrations and web service calls, both to and from Epic, is programmatically enforced. If an application attempts to access an incoming to Epic web service or subscribe to a Subspace event outside of its API scope, without a client ID or with an invalid client ID, the web service call or Subspace subscription will fail and the server or Subspace will return a forbidden error indicating insufficient scope. For outgoing web service calls from Epic, the associated client ID must be active in the customer's Epic system for the web service call to go to the external application successfully.

**Activating a Client ID**

For applications created with the open.epic FHIR developer toolbox, follow the app creation & request process to activate the client ID in Epic Community Members' Epic environments. These applications may use FHIR web services.

For applications that use Epic Public APIs, request a client ID from Epic by submitting an email request. When you are ready to test your interface with an Epic Community Member, have them reach out to their Epic representative to activate the client ID.

**Using a Client ID with Incoming to Epic Web Services**

The use of the client ID depends on your authentication method. OAuth2 is the recommended and most secure authentication available.

1. When using OAuth2, the client ID is used to retrieve an authorization code and access token. The access token is then used with subsequent web service requests and implicitly references the client ID. For more information on the OAuth2 workflow, please reference our OAuth2 tutorial.
2. If you cannot use OAuth2, the client ID must be included in the header of the web service request in one of the following ways:
    - In the HTTP header - see examples (available as an option for both REST and SOAP calls)
    - In the SOAP header (only an option for SOAP calls, not recommended)

For Subspace integrations, OAuth2 is required and the client ID is used to retrieve an access token. The access token is then used with Subspace subscriptions and implicitly references the client ID. For more information, please reference the Subspace specification.