**Azure API for FHIR**

In this hackathon we used the Azure API for FHIR to ensure the ability for WHO or a healthcare organization to integrate with their existing systems whilst guaranteeing security, compliance and adherence to each country’s regulations.

As this is a global pandemic, we wanted to provide a flexible, yet powerful set of tools to be easily deployed and managed in each location: More details can be found here:

<https://docs.microsoft.com/en-us/azure/healthcare-apis/>

For the hackathon we did not implement security protocols. We did not gather or use real patient data, only “ fake data” to test the features and functionality of the application.

**Azure Active Directory identity configuration for Azure API for FHIR**

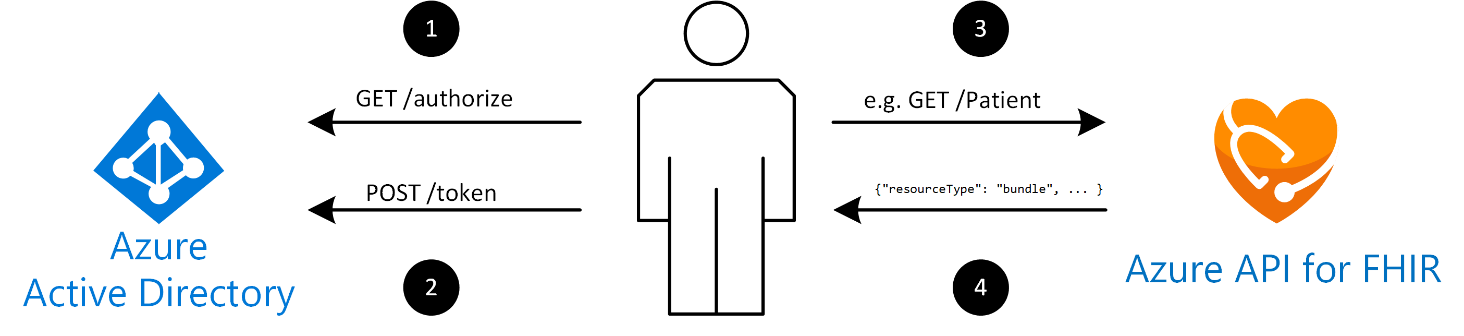
An important piece when working with healthcare data is to ensure that the data is secure and cannot be accessed by unauthorized users or applications. FHIR servers use [OAuth 2.0](https://oauth.net/2/) to ensure this data security. The [Azure API for FHIR](https://azure.microsoft.com/services/azure-api-for-fhir/) is secured using [Azure Active Directory](https://docs.microsoft.com/azure/active-directory/), which is an example of an OAuth 2.0 identity provider. This article provides an overview of FHIR server authorization and the steps needed to obtain a token to access a FHIR server. While these steps will apply to any FHIR server and any identity provider, we will walk through Azure API for FHIR as the FHIR server and Azure AD as our identity provider in this article.

**Access control overview**

In order for a client application to access Azure API for FHIR, it must present an access token. The access token is a signed, [Base64](https://en.wikipedia.org/wiki/Base64) encoded collection of properties (claims) that convey information about the client's identity and roles and privileges granted to the client.

There are a number of ways to obtain a token, but the Azure API for FHIR doesn't care how the token is obtained as long as it's an appropriately signed token with the correct claims.

Using [authorization code flow](https://docs.microsoft.com/azure/active-directory/develop/v1-protocols-oauth-code) as an example, accessing a FHIR server goes through the four steps below:



1. The client sends a request to the /authorize endpoint of Azure AD. Azure AD will redirect the client to a sign-in page where the user will authenticate using appropriate credentials (for example username and password or two-factor authentication). See details on [obtaining an authorization code](https://docs.microsoft.com/azure/active-directory/develop/v1-protocols-oauth-code#request-an-authorization-code). Upon successful authentication, an *authorization code* is returned to the client. Azure AD will only allow this authorization code to be returned to a registered reply URL configured in the client application registration (see below).
2. The client application exchanges the authorization code for an *access token* at the /token endpoint of Azure AD. When requesting a token, the client application may have to provide a client secret (the applications password). See details on [obtaining an access token](https://docs.microsoft.com/azure/active-directory/develop/v1-protocols-oauth-code#use-the-authorization-code-to-request-an-access-token).
3. The client makes a request to the Azure API for FHIR, for example GET /Patient to search all patients. When making the request, it includes the access token in an HTTP request header, for example Authorization: Bearer eyJ0e..., where eyJ0e... represents the Base64 encoded access token.
4. The Azure API for FHIR validates that the token contains appropriate claims (properties in the token). If everything checks out, it will complete the request and return a FHIR bundle with results to the client.

It is important to note that the Azure API for FHIR isn't involved in validating user credentials and it doesn't issue the token. The authentication and token creation is done by Azure AD. The Azure API for FHIR simply validates that the token is signed correctly (it is authentic) and that it has appropriate claims.

<https://docs.microsoft.com/en-us/azure/healthcare-apis/azure-ad-hcapi>