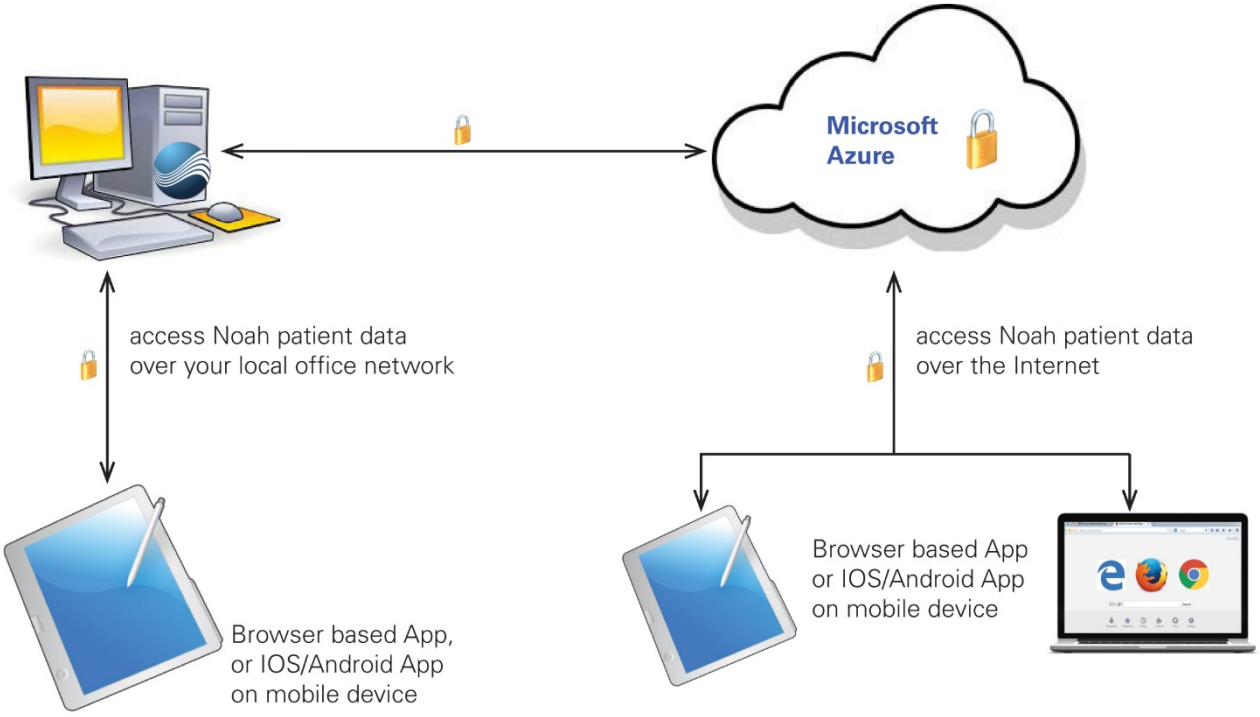
White Paper

What is Noah Mobile technology?

Noah Mobile technology, included with Noah, implements a platform independent Web API which lets you work with your patients on mobile devices such Android tablets and iPads and internet browser-based applications.

With Noah Mobile, mobile and browser-based apps from HIMSA and HIMSA member companies will be able to easily interact with Noah, just like Windows based modules do today.



For example, with Noah Mobile technology you could use an app to:

- Establish a secure connection to your Noah server, either from within your office or at a remote patient site
- Search for and open a patient's data record
- Perform patient activities such as a fitting, a measurement or a questionnaire
- Store the new patient data in the Noah database when you are done

And since each Noah Mobile app communicates directly with Noah System on your PC, there's no need to install Noah System on your mobile device.

Who can make a Noah Mobile app?

Only HIMSA and HIMSA member companies can make Noah Mobile apps.

What kinds of apps are available?

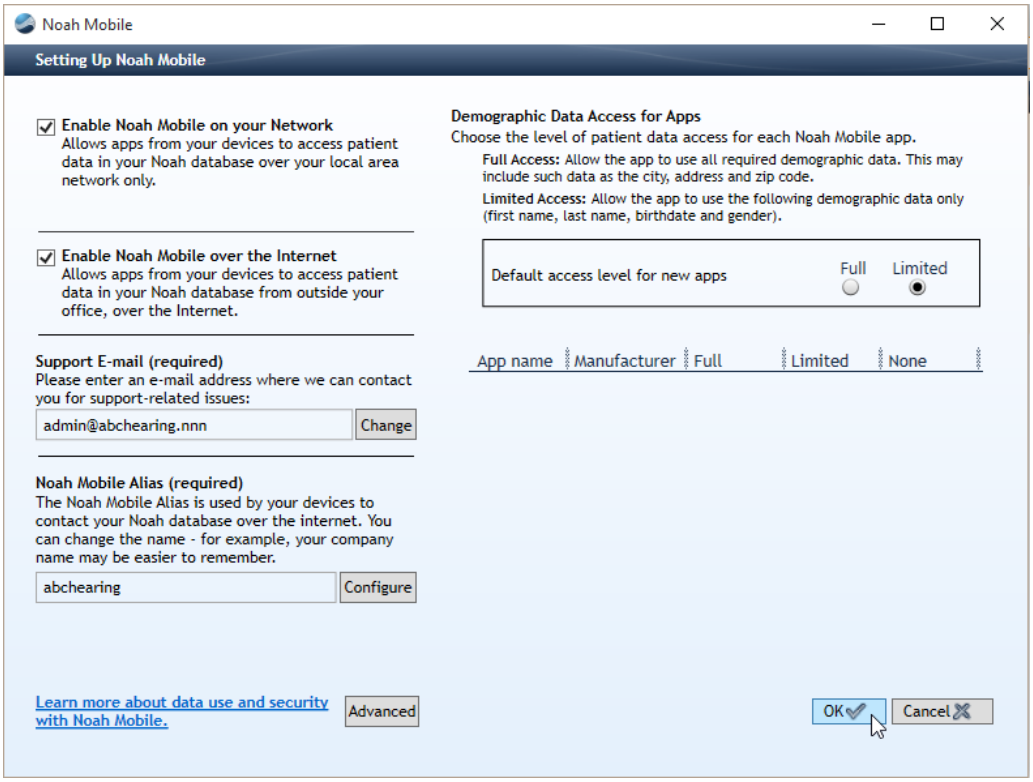
Our member companies are free to decide the best types of Noah Mobile apps to provide and which mobile devices to support.

Potentially these apps can include everything from fitting and measurement apps to journal and questionnaire apps, ordering apps, telemedicine apps and more.

All HIMSA-certified Noah Mobile apps are listed on the HIMSA website www.himsa.com.

Can I control which apps can access my Noah data?

Yes, your Noah administrator has control over which apps can access your patient data and how much patient data they can access.



Your administrator can also choose to disable Noah Mobile access at any time if your business no longer wishes to use Noah Mobile apps.

Does my data need to be stored on the internet for Apps ussing the Web API (Noah Mobile)?

No, HIMSA does not need host any patient data on the Internet; all data remains stored in your Noah database.

Noah Mobile technology only provides a secure relay service between your Noah database and your Noah Mobile apps.

Microsoft Azure

Noah Mobile currently uses two Microsoft Azure datacenters – Western EU and Central US. Each Noah installation is associated with one of these data centers and the data will always be transmitted via the associated data center.

For a detailed technical description of how Azure is used by the Noah Mobile Cloud Service, please refer to our whitepaper on *How Noah Mobile uses Microsoft Azure Core Services*.

Cost of Internet use

The use of the Internet connection must be provided by your practice. Keep in mind that if you are using a metered connection it can be quite expensive.

Data security

HIMSA's use of data

HIMSA will not read or collect information on patient related data. In fact, it is not technically possible for HIMSA to see or comprehend the data as it is transferred between Noah and an app.

Noah does store an address identifier for your Noah server network in the secure Microsoft Azure environment. Noah uses this IP address information so that apps know how to connect to Noah via encrypted, certificate based connection methods.

App access to patient data

HIMSA provides the following rules to ensure the proper use of patient data by Noah Mobile apps:

- Your Noah administrator must first grant access before an app can connect to Noah. Your Noah administrator can also specify the level of demographic data that can be seen by the app.
- Once an app has access, employees in your office will still need to provide a valid Noah user name and password in order to use the app. For best data security, we suggest that each individual Noah user in your office uses their own username and password. You should enable the use of strong passwords for all Noah users.
- App developers are required via HIMSA license agreements to obtain HIMSA certification for each released version which also requires a clearly written explanations from the App supplier on how they are able to utilize patient related data gained via Noah. While HIMSA is not responsible for any infractions performed by app developers, we will react to known violations.

- Apps may have access to patient related data in order to provide the features requested by the user. However, after the app is finished with the requested work, it is required to permanently remove the data from the app and not use the data in the future unless the user requests additional interaction. If the app developer offers additional services that necessitate that data is copied to another application or location, the app developer must clearly notify the user of this.
- For added security, Noah provides an audit trail feature which automatically records data activity per user and app. This data can be viewed by your Noah administrator at any time.

Secure patient data communication

All communication with the Noah Mobile solution uses transport layer security (TLS) to protect communication between the client and the service as well as the cloud service and the remote hosts.

Transport layer security is also used for all communication with internal services within the cloud service.

- **Communicating on your office network:** If you are using Noah Mobile to access patient data over your office network, Noah Mobile will need an Internet connection to verify your Noah server address. However, no patient data will be sent outside your office over the Internet.
- **Communicating over the Internet:** If you are working outside of your office, Noah Mobile will rely on Microsoft Azure to securely exchange patient data over the Internet, helping to ensure that only the requesting app can see the patient data.

Noah Mobile provides the following security features.

Encrypted Communication – Noah Mobile relies on encryption to protect the communications at all steps between the app and Noah.

Authorization – Noah Mobile supports OAuth 2.0 Authorization, and requires that apps are authorized to access your Noah data. This authorization occurs when an employee from your office connects to your Noah server from the app and enters their Noah login information. By using OAuth, the app never has access to the Noah users' user name and password.

A successful Authorization will return an Access Token which will allow the app to access data on your Noah server. If the app remains inactive for an extended period, it is required to automatically disable the token to avoid unwanted access to your Noah patient data.