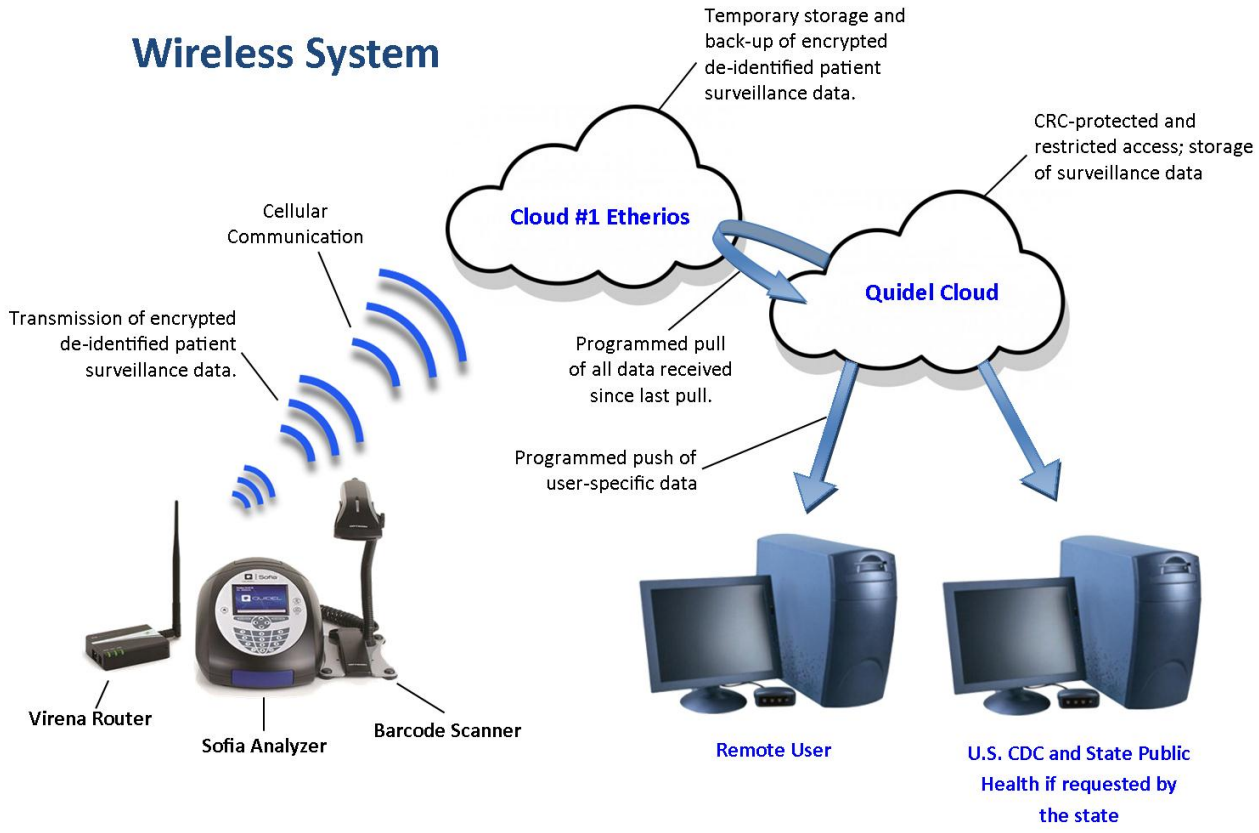
Security for Each Element in Communication Path

Figure below indicates the communication path of data information between the Sofia®, Virena (Digi) Router, and Quidel cloud-based system.



Sofia to Virena (Digi) Router

Sofia generates a message containing a patient, QC or calibration result. This message contains a few header bytes which include instrument type, in this case the code for Sofia, and the analyzer serial number. The remainder of the message contains the data elements which are encrypted as a single data package using a proprietary encryption algorithm. The encryption is maintained until the message is received in the Quidel Cloud where it is decrypted.

It is assumed that the Sofia and Virena router are connected by Ethernet, either a direct connection or over the site's local area network (LAN), and as such data security via LAN is the user's responsibility.

Virena Router to Etherios Cloud (formerly iDigi Cloud)

The Virena router communicates with the Etherios Cloud via cellular wireless or the Internet. The result files are double encrypted. The data within the file is encrypted as described above and the file is transmitted using SSL.

Etherios Cloud

The Etherios Cloud is a web-based service access point for all M2M data and management activities. As a web-service, the connection between the enterprise application and the Etherios Cloud takes place over the public Internet. The security strategy employed in this domain is one with a long and well-proven track record: authentication and data encryption are handled by using the Secure-Sockets Layer ("SSL") over HTTP, also known as HTTPS. Authentication will prove the identity of each side but it does nothing to keep data save from eavesdroppers. The SSL transport provides a secure link safe from prying eyes using strong, negotiated public-key encryption.

Security of the Etherios Cloud is described in the attached link:

http://www.etherios.com/pdf/tb_devicecloudsecurity.pdf

The Quidel Cloud normally polls the Etherios Cloud once per day at 08h00 UTC and downloads all result files. After authentication and loading to the Virena database, result files on the Etherios Cloud are deleted. Although the Etherios Cloud is a secure environment, this approach ensures results are saved in the Etherios Cloud for less than 24 hours.

Etherios Cloud to Quidel Cloud

The Virena application is hosted in the Microsoft Azure Cloud service. Security is described in the attached link:

http://azure.microsoft.com/en-us/support/trust-center/security/

Incoming results from the Etherios Cloud are decrypted and checked for validity. Result files that do not meet acceptance criteria are saved to an exceptions file for review by the Quidel System Administrator. Files that are valid are entered in the Virena database and other data elements such as Organization, Facility, LOINC codes and SNOMED codes are added. The result files in the Etherios Cloud are deleted.

Quidel Cloud – Results Export

Results may be exported in a csv format to a sftp or ftp site. Such transmission also uses SSL. This export takes place once per 24 hours and the task needs to be set up by the Quidel System Administrator.

Quidel Cloud – Web Access

Access to "MyVirena.com" requires both a valid user name and password. Quidel System Administrator grants this access after receipt of a written application and approval of the Organizations designated responsible person. Once logged in, security is maintained using SSL, Symantec is the Certificate Authority.