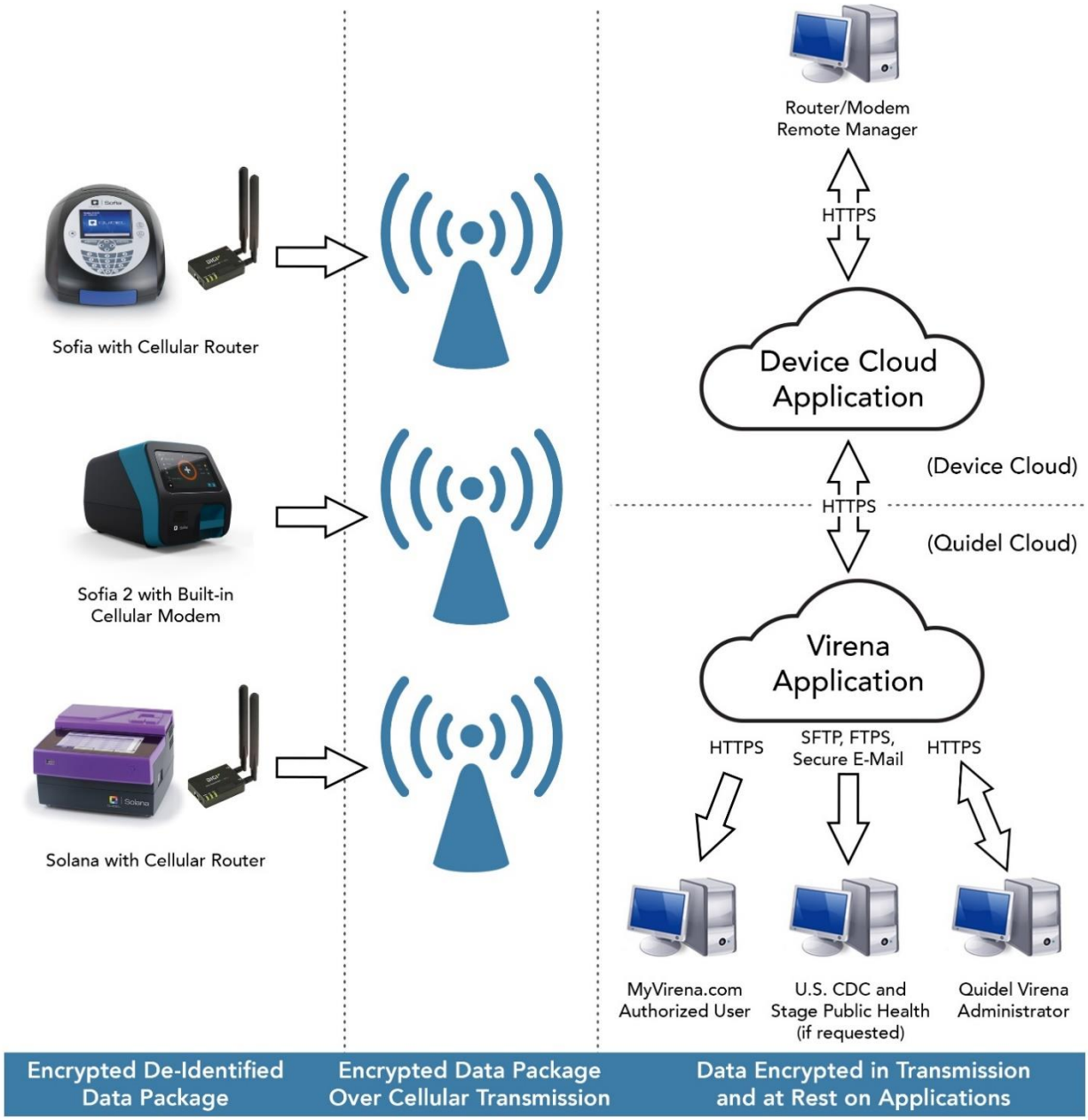
Cybersecurity Overview

This document describes the standards and controls established by Quidel on the Virena System Platform and answers common cybersecurity questions.

Figure 1: Virena System Platform Diagram



The Quidel Virena System Platform (Figure 1) consists of (1) Quidel Instrument, (2) Digi Cellular Router/ Modem, which are located at the customer site, (3) Cellular transmission to transmit data, (4) Digi Device Cloud, which manages the router connectivity and stores the forwarded data temporarily, and (5) the Quidel Cloud, which houses the Quidel Virena Application. Standards and security controls for each element of the platform process are described on the next page.

1. Quidel Instrument

Your Quidel Instrument generates a message containing de-identified, QC or calibration data with no protected health information (PHI). The message contains header bytes, which include instrument ID, Cassette serial number and the data length of the encrypted package. The remainder of the message contains the data elements, which are encrypted by the Quidel instrument as a single data package before it is sent to the Cellular Router/Modem. The Quidel Instrument software ensures only one-way transmission occurs from the Quidel Instrument to the Cellular Router/Modem. Quidel encryption is maintained end-to-end beginning with the Quidel Instrument until the message is received in the Quidel Cloud, where it is decrypted by the Quidel Virena Application.

2. Cellular Router/Modem

The Cellular Router/Modem receives the data package from the Quidel Instrument. The data packages are transmitted using SSL with Quidel encryption that is already present on the package. The Router/ Modem SSL encryption is maintained over cellular transmission until it is received in the Device Cloud where it is decrypted, thus providing additional data security. Quidel currently utilizes Digi to provide Cellular Routers/Modems.

3. Cellular Transmission

Cellular transmission of the data package occurs using standard cellular providers. Encryption is maintained on the data package throughout the transmission from the Digi Cellular Router to the Digi Device Cloud.

4. Device Cloud

The Device Cloud is a web-based service access point for all Quidel data packages, which are received from the Router/Modem over cellular transmission. Data package encrypted by the Router/Modem are decrypted and stored temporarily in the Device Cloud. At this point, Quidel encryption is still maintained on the package. The Device Cloud is also used to setup and maintain the Routers/Modems using a Remote Manager application by Quidel authorized personnel. Compliance standards and cybersecurity controls on the Device Cloud are explained here: https://www.digi.com/pdf/tb_devicecloudsecurity.pdf

5. Quidel Virena Application

The Quidel Virena application polls the Device Cloud frequently and downloads all data packages. After authenticating and loading the data packages to the Virena application database, the data packages on the Device Cloud are erased. The data packages received by the Virena Application are decrypted and checked for validity, thus maintaining end-to-end secure encryption from Quidel Instrument to Quidel Virena Application. Data packages that are valid are entered in to the Quidel Virena Application database with assigned and matched data elements such as Organization, Facility, LOINC codes and SNOMED codes. Quidel Virena Application data is encrypted at rest. Data packages that are not valid (including PHI) are erased and not entered into the Quidel Virena Application.

Quidel Customers access the Virena Web Application “MyVirena.com” using HTTPS, which requires a valid user name and password. A Quidel authorized System Administrator grants the access after receiving an approved written request from the customer’s designated authority. The Quidel Virena Application is hosted on Microsoft Azure Cloud service. Microsoft Azure’s Cybersecurity Standards and Controls are explained here: https://www.microsoft.com/en-us/trustcenter/security/azure-security

When requested, data is available through secure processes to authorized public agencies.