Introduction

This document describes the PHI collection and storage of Cognivue Clarity and Thrive. It also provides details on the security measures on the device.

PHI Collection and Storage

Cognivue Clarity and Thrive collect and store the following information on a per-test basis:

- Patient's first name, middle initial, and last name.
- Patient's date of birth
- Patient's gender
- Patient's subtest scores and domain scores.
- (Optionally) Patient's email.

Cognivue Clarity and Thrive store information on the device in a Postgres database that is only accessible from on-device processes.

As part of the screening process, the device also generates a report which contains this information.

Administrators can set up a network file share to access the directory where the reports are stored.

A device administrator can also configure the device to create an HL7 message that holds the listed PHI.

Device Security

As part of our responsibility to comply with the FDA's guidance on medical device cybersecurity and HIPAA regulations, the device has several security features in place.

- The device is managed and monitored by the AWS Systems Manager tool. This tool enables our team to resolve issues remotely; Systems Manager uses HTTPS to communicate.
- The on-device firewall blocks all incoming and outgoing connections except for the ones needed for the file share. (Administrators can find details at Firewalling Samba)
- Cognivue Clarity/Thrive uses HTTPS for all outgoing and incoming network traffic.
- Access to the underlying OS (Ubuntu 18.04 LTS) is not permitted except for limited operations.
    - These include network and printer configuration.
    - The device can use a printer connected by USB or a network at will.
- The OS receives security updates automatically.
- The system has an AV solution, ClamAV, installed and running.

- The folder share requires a password that the device administrator (Admin) can change.
- Device administrators are the only user that view reports on the device.
- Operator users can view the test reports immediately after the test concludes but cannot view older reports on the device.
- Device administrators can enable user account password expiration.
- The device can hide all reports from tests administered before a specific date.
    - This action does not delete the database results; however, it removes the reports from the Reports folder and hides the corresponding test session from the UI.