HEART use case involving remote patient monitoring device
Sharing pulse oximeter data in a consented way with third parties

The following use case is illustrated with screenshots from a demonstration that was implemented using the ForgeRock Identity Platform, Qualcomm Life’s 2Net Services, and a Nonin 2320 pulse oximeter device.

1. Dr. Lopez prescribes a pulse oximeter to Lynda Wallace; an administrator provisions it electronically.

2. When Lynda first logs in to the ACME Medical patient portal, her device is inactive.
3. After she clicks on the red light, she is asked to consent to device activation and data reading by Dr. Lopez

4. After she consents, her device now shows as active, meaning a policy is lodged to allow data sharing and her smartphone is prepared to be a hub
5. After pairing the oximeter device to her phone, she logs in to her ACME Medical mobile app using the same identity credentials as on the portal.

6. The mobile app securely mediates an oximeter data reading, and shows that the reading was successful.
7. Dr. Lopez logs in to the ACME Medical portal

8. Dr. Lopez’s view once authenticated is this home screen

9. In his My Patients view, Dr. Lopez sees a listing with Lynda Wallace and others
10. Dr. Lopez selects Lynda Wallace as the patient whose data he wants to view.

11. He chooses Lynda’s device profile.
12. Because of the policy she consented to activate, Dr. Lopez is able to proceed to view her data.

Some background: HEART profiles the User-Managed Access (UMA) 2.0 grant of OAuth, which: a) gives Dr. Lopez’s client app a permission ticket on first resource attempt; b) requires an ID token for proof; c) issues an access token; and d) requires it for data access.