High summarization of Kantara UMA 2.0: User-Managed Access

First delivered by Eve Maler. ForgeRock, @xmlgrrl & Mike Schwartz, Gluu, @gluufederation 27 June 2018

gluu

FORGEROCK

User-Managed Access has important implications for those facing regulatory pressures around data protection, market pressures around consumer trust, and architectural pressures around API protection.

The following slides will offer a very high level overview of the context, purpose, structure, and flows of the UMA 2.0 protocol, including its OAuth2 extension grant and its federated authorization API.

The UMA standard's progress

2015

Mar '15: UMA V1.0 ratified as Recommendations

2016

Dec '15: UMA V1.0.1 ratified as Recommendations

2017

Specs refactored, over 100 issues closed, lots of implementation input received, Disposition of Comments doc written…

Jul '17: 1st Public Comment/ Review period ends

Sep '17: 2nd Public Comment/ Review period ends

2018

Jan '18: UMA2 logo (designed by @domcat)

Jan '18: Final Recommendations published

Jan '18: Draft UMA Business Model Report published

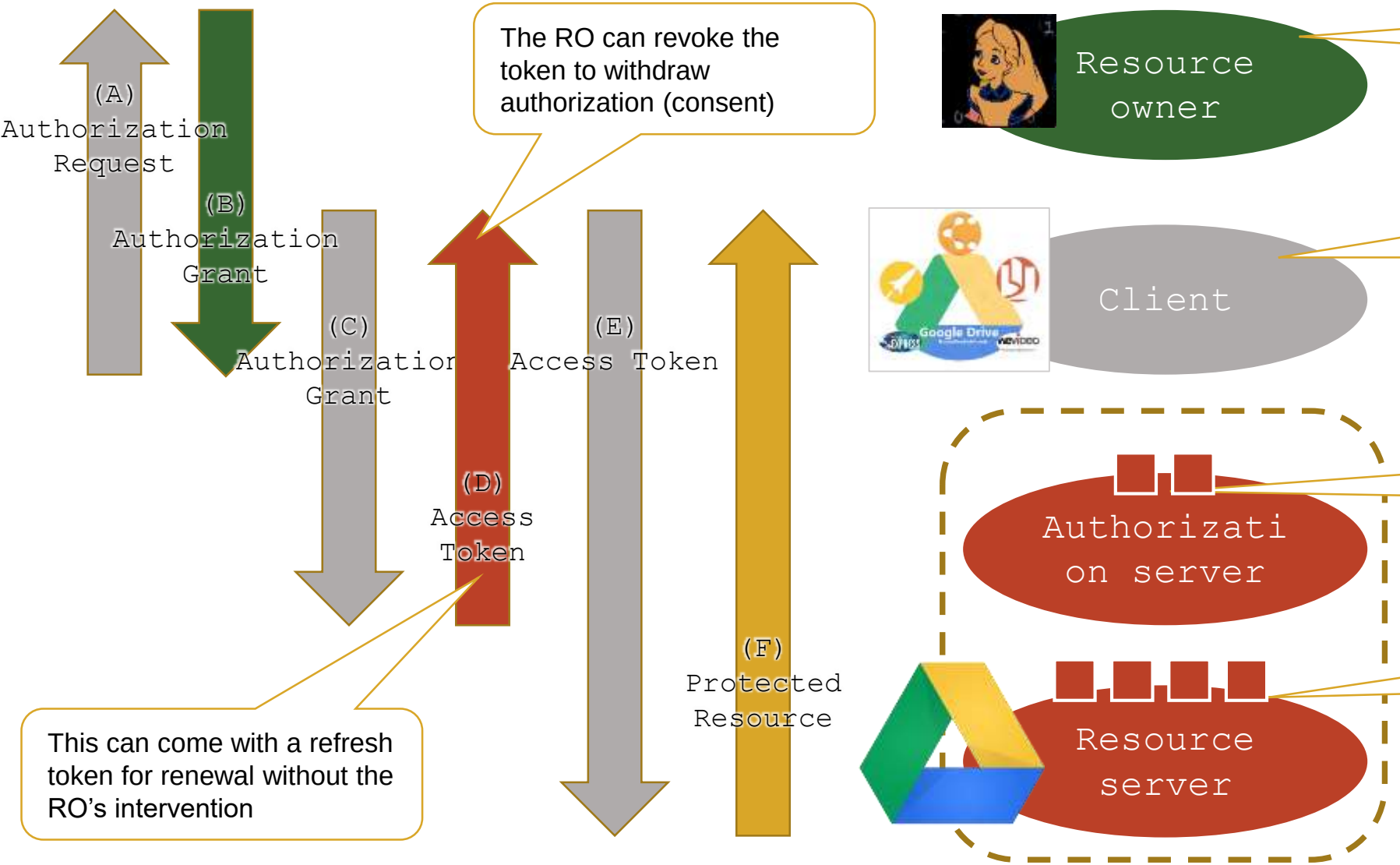
Feb '18: Charter update

May '18: Vendors supporting UMA2: Gluu, ForgeRock, Keycloak (WSO2 coming Q3)

Jun '18: Business model/ IRM cxn jells

OAuth is for constrained delegation to apps

It has helped to kill the “password anti-pattern”



The RO can revoke the token to withdraw authorization (consent)

This can come with a refresh token for renewal without the RO’s intervention

Authorizes (consents) at run time after authenticating, at the AS

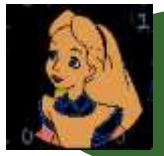
App gets consent based on the API scopes it requested; it has its own identity distinct from the RO’s

Standard OAuth endpoints for authorization and access token issuance

Some number of API endpoints that deliver the data or other value-add

OpenID Connect does modern-day federation

It is an OAuth-protected identity API, plus a bit more



Resource owner = Federation user

Client = Relying party

Along with access and refresh token, this endpoint also typically delivers an “ID token” similar to a SAML assertion

Authorization server

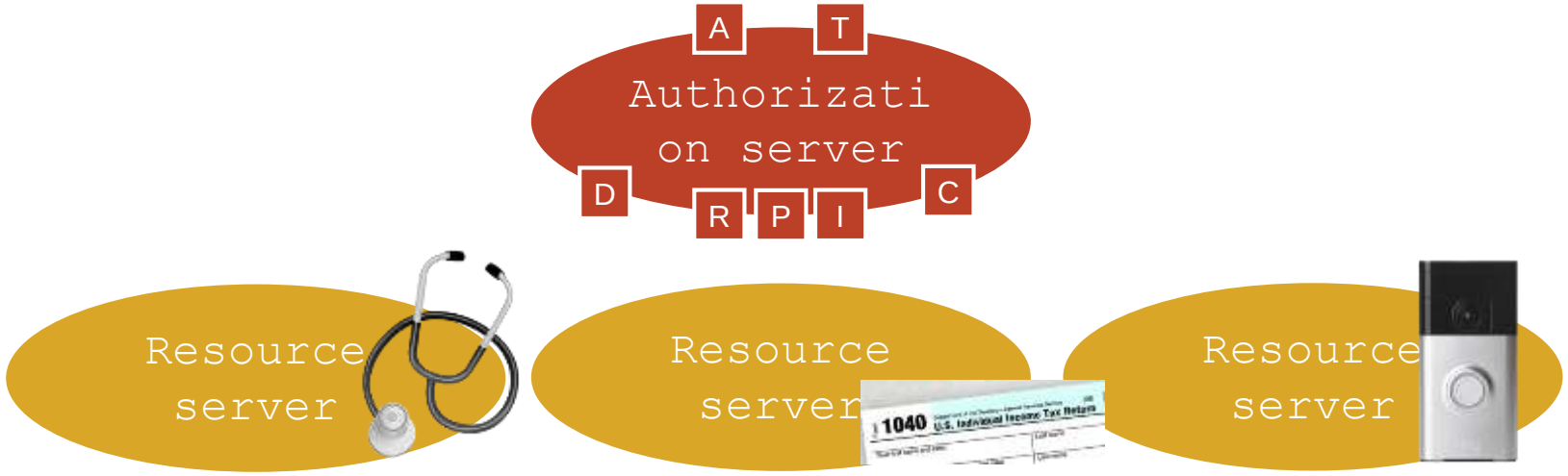
Resource server

= Identity provider (“OpenID provider”)

Standard UserInfo endpoint can be called with an access token to look up identity claims

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth



tinyurl.com/umawg
@UMAWG

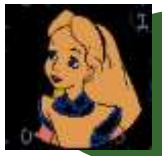
kantara INITIATIVE

UMA2

A authorization T token D discovery R resource registration P permission I token introspection C claims interaction

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth



Resource owner

Requesting party

Client

UX

Ahead of time	Anytime	Anytime	At run time	After the fact
Share	Monitor	Withdraw	Opt in	Approve

A T

Authorization server

D R P I C

Resource server

Resource server

Resource server

tinyurl.com/umawg
@UMAWG

A authorization T token D discovery R resource registration P permission I token introspection C claims interaction

Like OpenID Connect for *identity*, UMA adds an API *access management* layer to OAuth2

Some use cases for UMA:

- Enterprise API protection
- For financial consumers
  - Discovering and aggregating UK pension accounts and sharing access to financial advisors
- In industrial and consumer IoT
  - For proactively or dynamically sharing smart device control or data with others
- Healthcare
  - As profiled in the Health Relationship Trust (HEART) WG at OpenID Foundation
  - Part of the new OpenMedReady framework for trustworthy remote care

ORIGO

Alongside Open APIs, **UMA would enable consumers to have full control of who can access their data and for how long** – granting access for example, to their **financial adviser** or the Single Financial Guidance Body – as well as the ability to revoke access and for security to be in place to prove who is accessing the data. The UMA approach to security and consent is also well aligned with the requirements of GDPR (General Data Protection Regulations).

To sum up: UMA enhances OAuth as follows

The UMA2 Grant spec adds to OAuth2

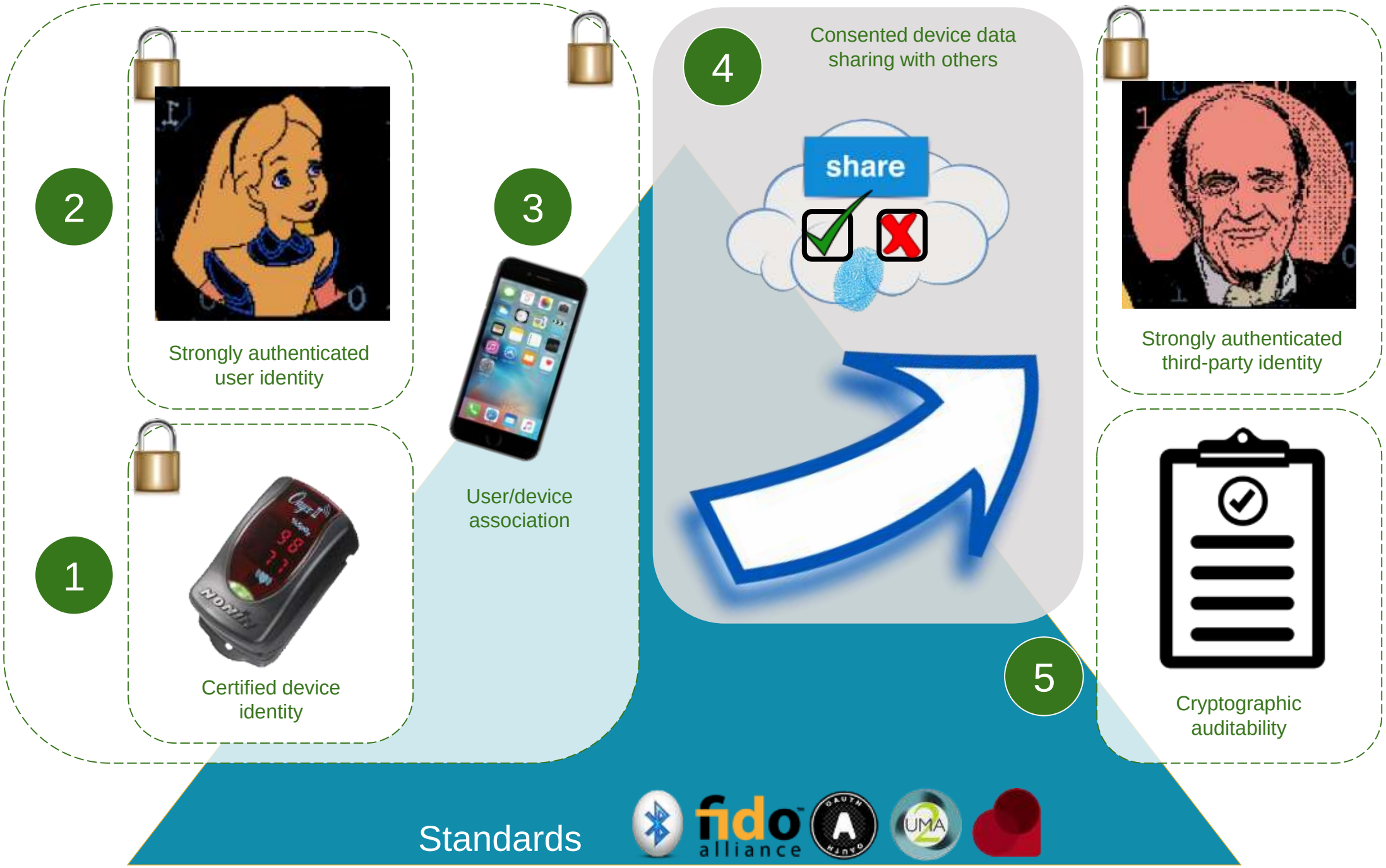
- The resource owner authorizes protected resource access to clients used by entities that are in a requesting party role. This enables **party-to-party authorization**, rather than authorization of application access alone.
- The authorization server and resource server interact with the client and requesting party in a way that is **asynchronous** with respect to resource owner interactions.
- This lets a resource owner **configure an authorization server with policy conditions at will**, rather than authorizing access token issuance synchronously just after authenticating.

The UMA2 Federated Authorization spec adds to the UMA2 Grant

- **Multiple** resource servers operating in different domains can communicate with a **single** authorization server operating in yet another domain that acts on behalf of a resource owner.
- A service ecosystem can thus automate resource protection, and the **resource owner can monitor and control** authorization grant rules through the authorization server over time.
- Authorization grants can **increase and decrease** at the level of individual resources and scopes.

Walkthrough by Eve:

Sharing pulse oximeter data in a trusted and consented way with third parties through loosely coupled cloud services


2
Strongly authenticated user identity
3
User/device association
4
Consented device data sharing with others
share
Strongly authenticated third-party identity
1
Certified device identity
5
Cryptographic auditability
Standards
fido alliance
UMA

Chrome File Edit View History Bookmarks People Window Help 62% Thu 1:09 PM Alex Lopez

OpenIDM | ForgeRock Access Manageme | Welcome to the ACME Medica

Not Secure https://openidm.aeet.fridam.aeet-forgerock.com/admin/#resource/managed/TwoNetDevice/edit/5a43e24f-69b8-413d-a233-9c730d3b2fc4

2NET DEVICE

Nonin 3230 - Lynda Wallace

Delete

1

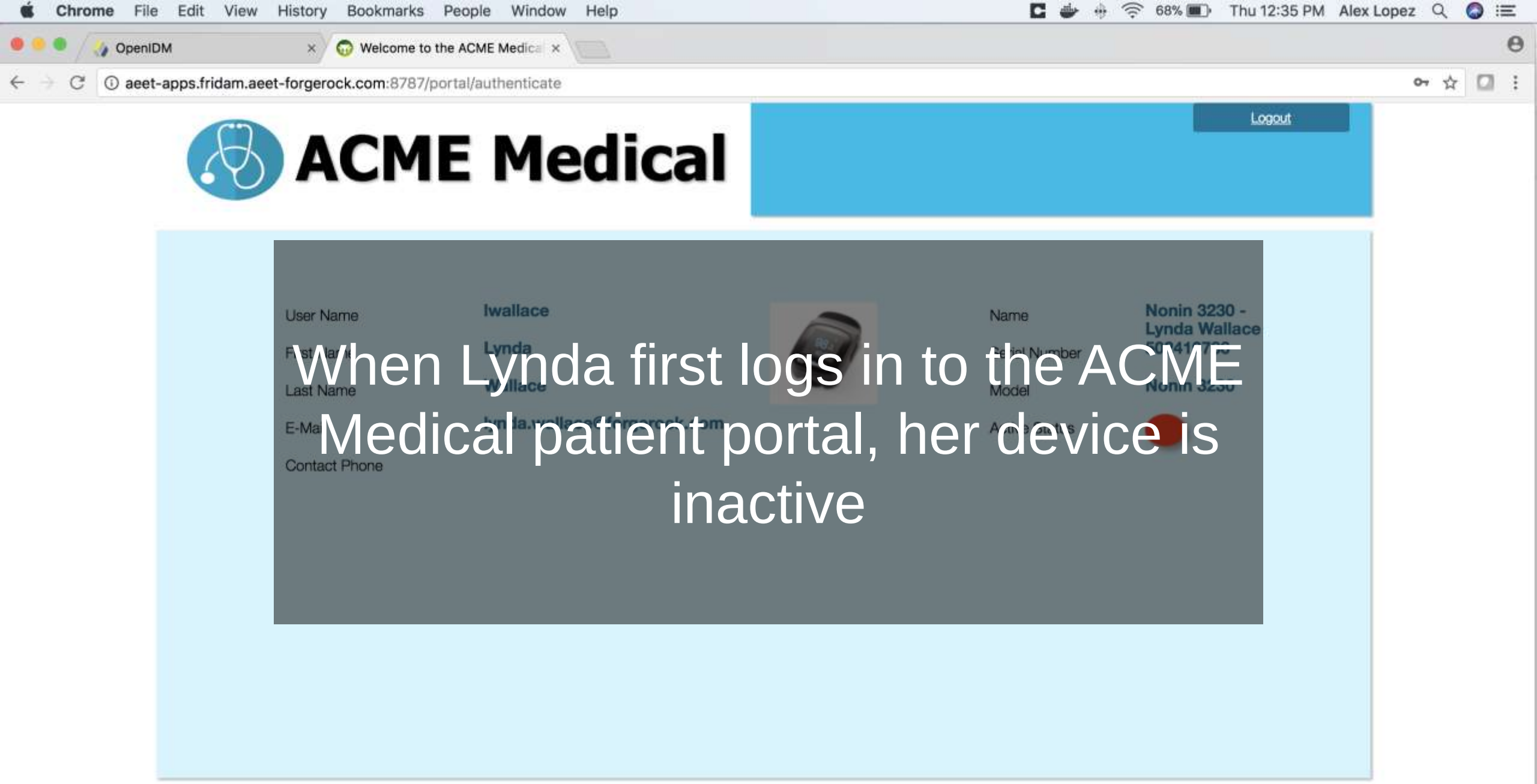
2

3

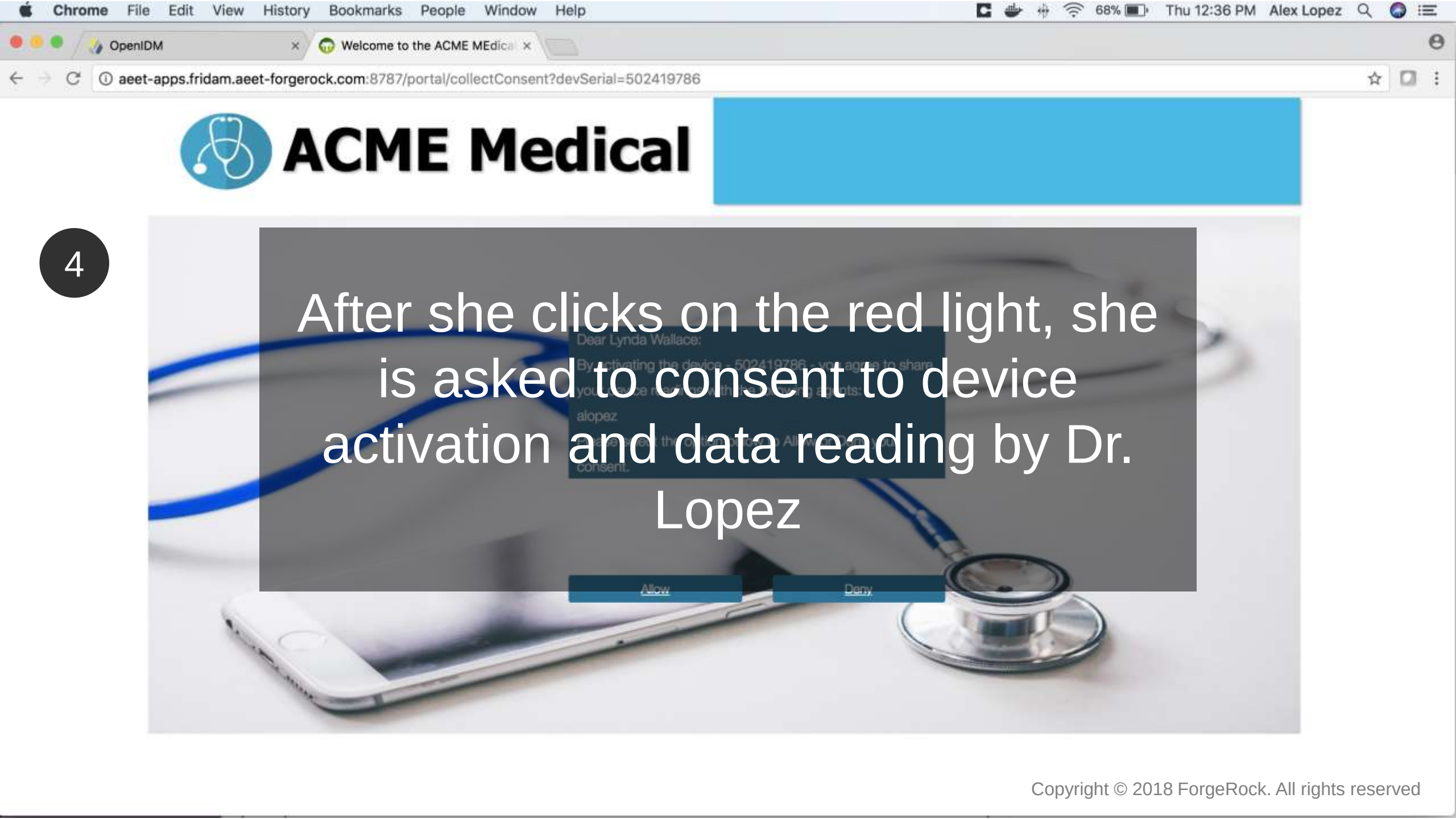
Details | DeviceReadings

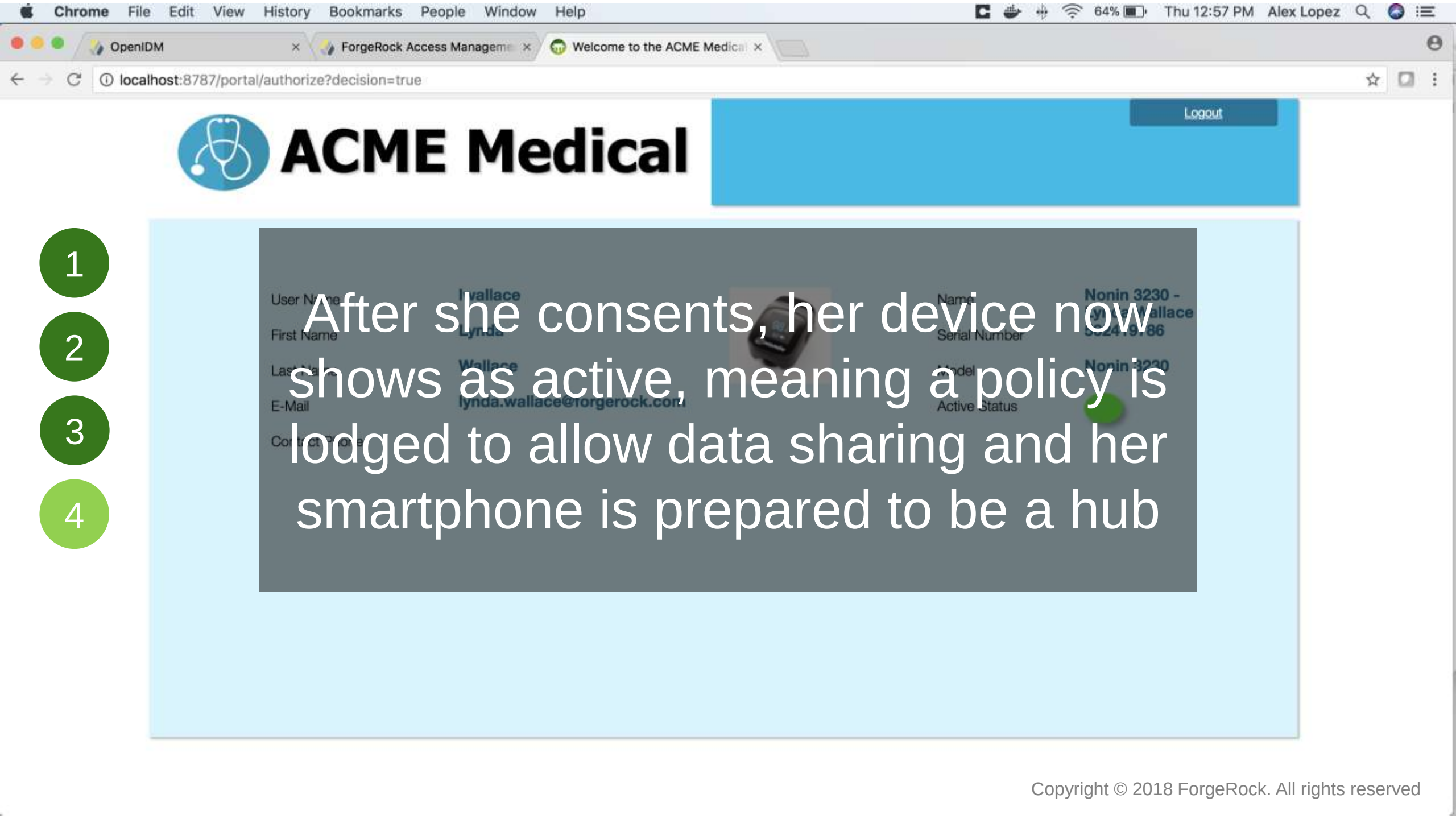
Dr. Lopez prescribes a pulse oximeter to Lynda Wallace; an administrator provisions it electronically

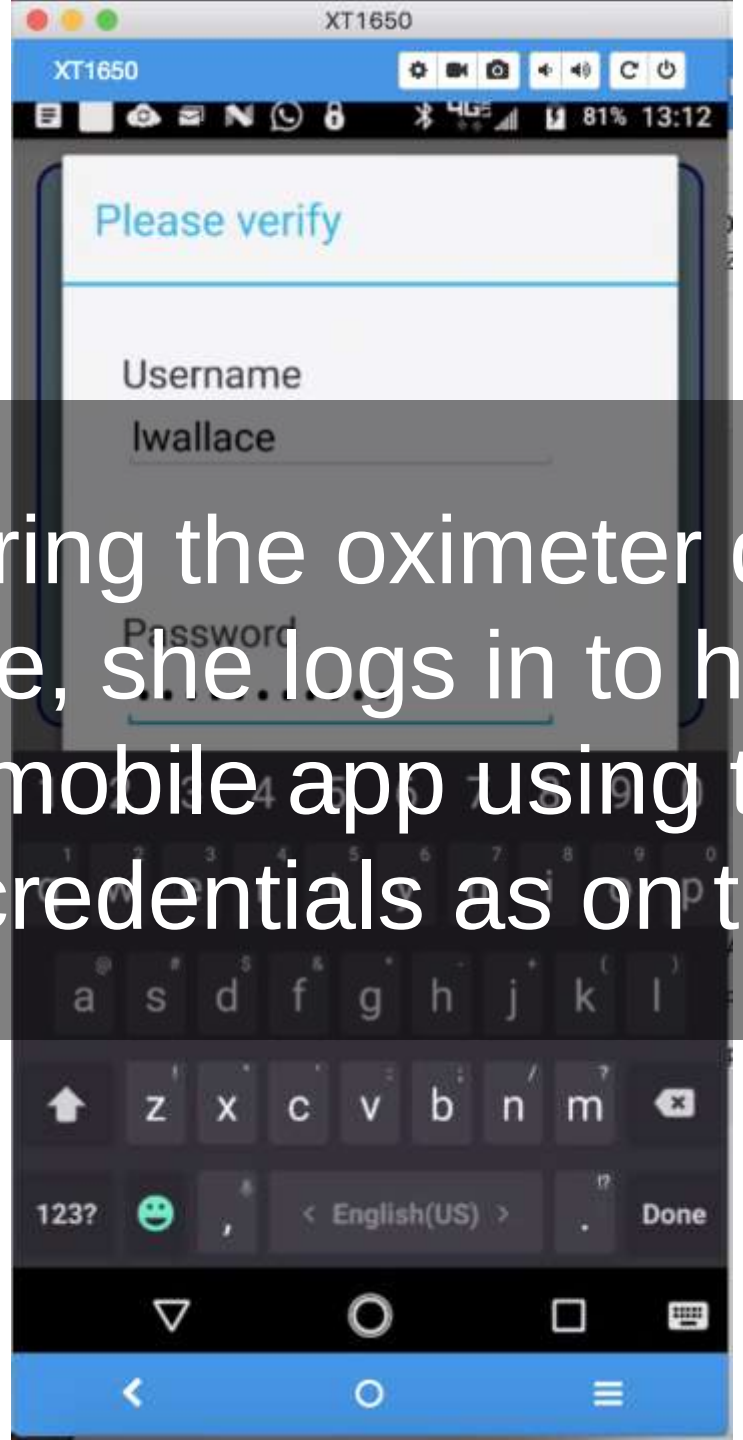
Name	Nonin 3230 - Lynda Wallace
Serial Number	5[illegible]
MAC Address	00:1C:05:FF:35:A8
Virtual Hub ID	FORGE001V0009765
Owner	Lynda, Wallace, lwallace · Update Owner · Remove Owner
Active Status	true
Device Model	Nonin 3230
UMA Resource ID	e6716120-b22a-4b59-9c17-b95a44c4ba2f0
UMA Resource Owner Credentials	llohcbe2107



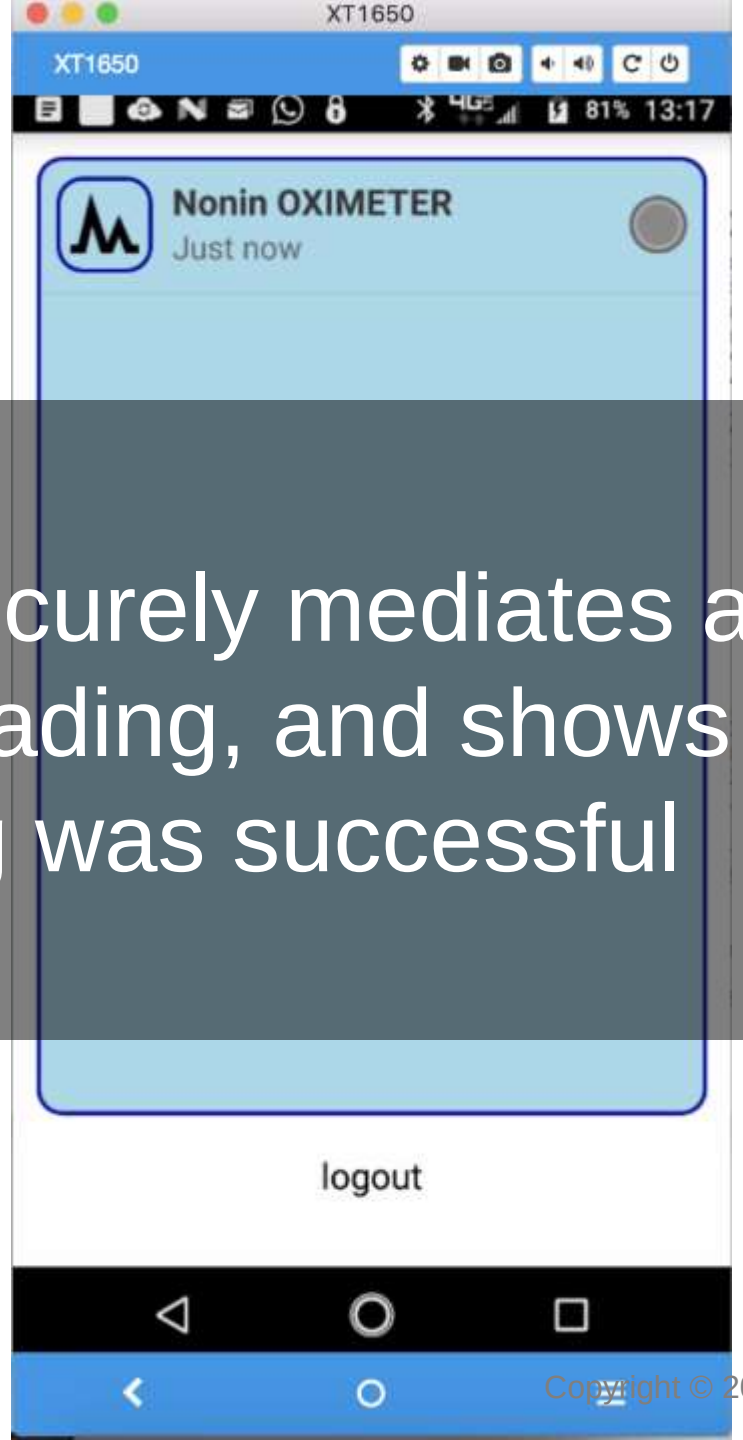
When Lynda first logs in to the ACME Medical patient portal, her device is inactive



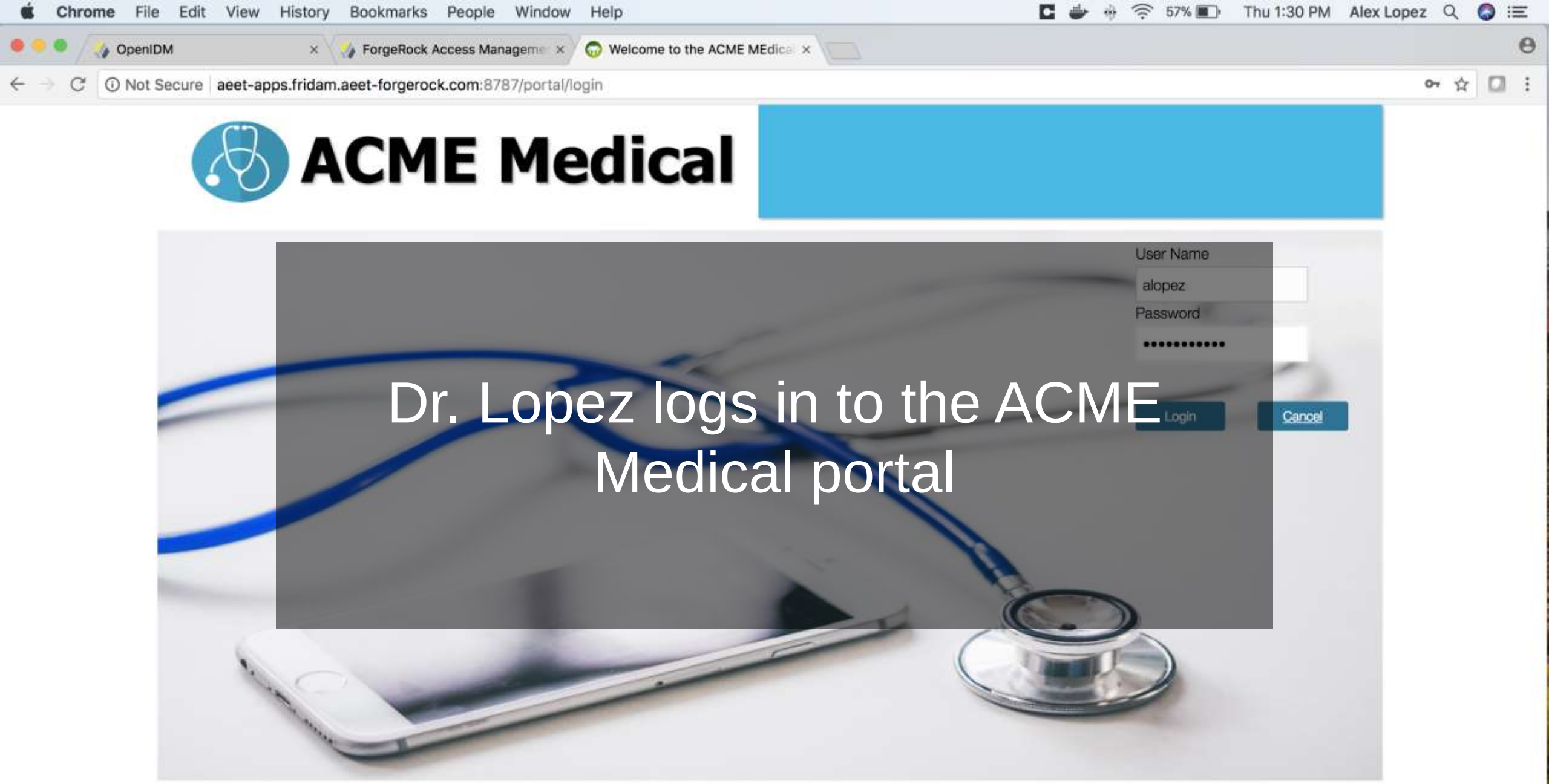




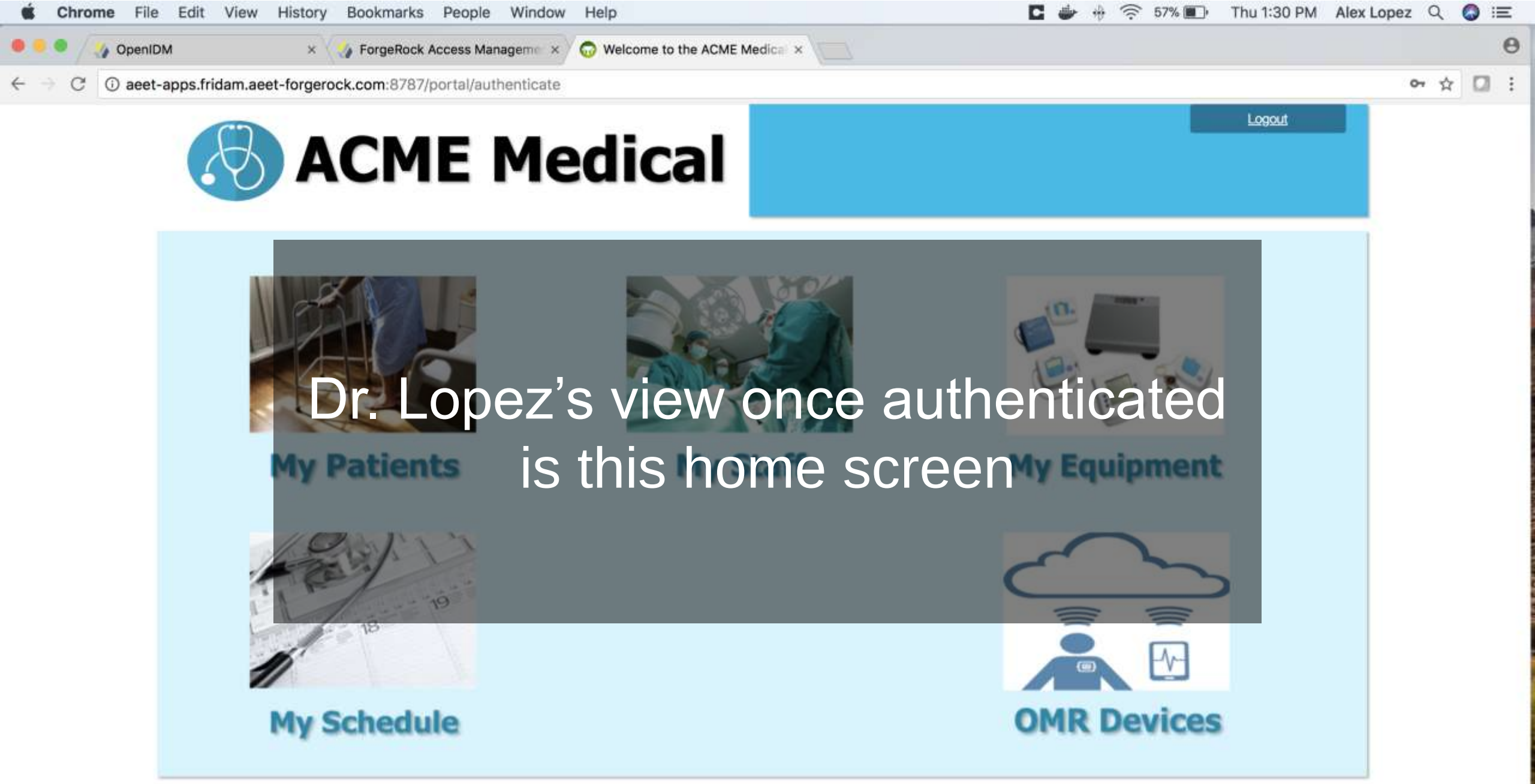
After pairing the oximeter device to her phone, she logs in to her ACME Medical mobile app using the same identity credentials as on the portal



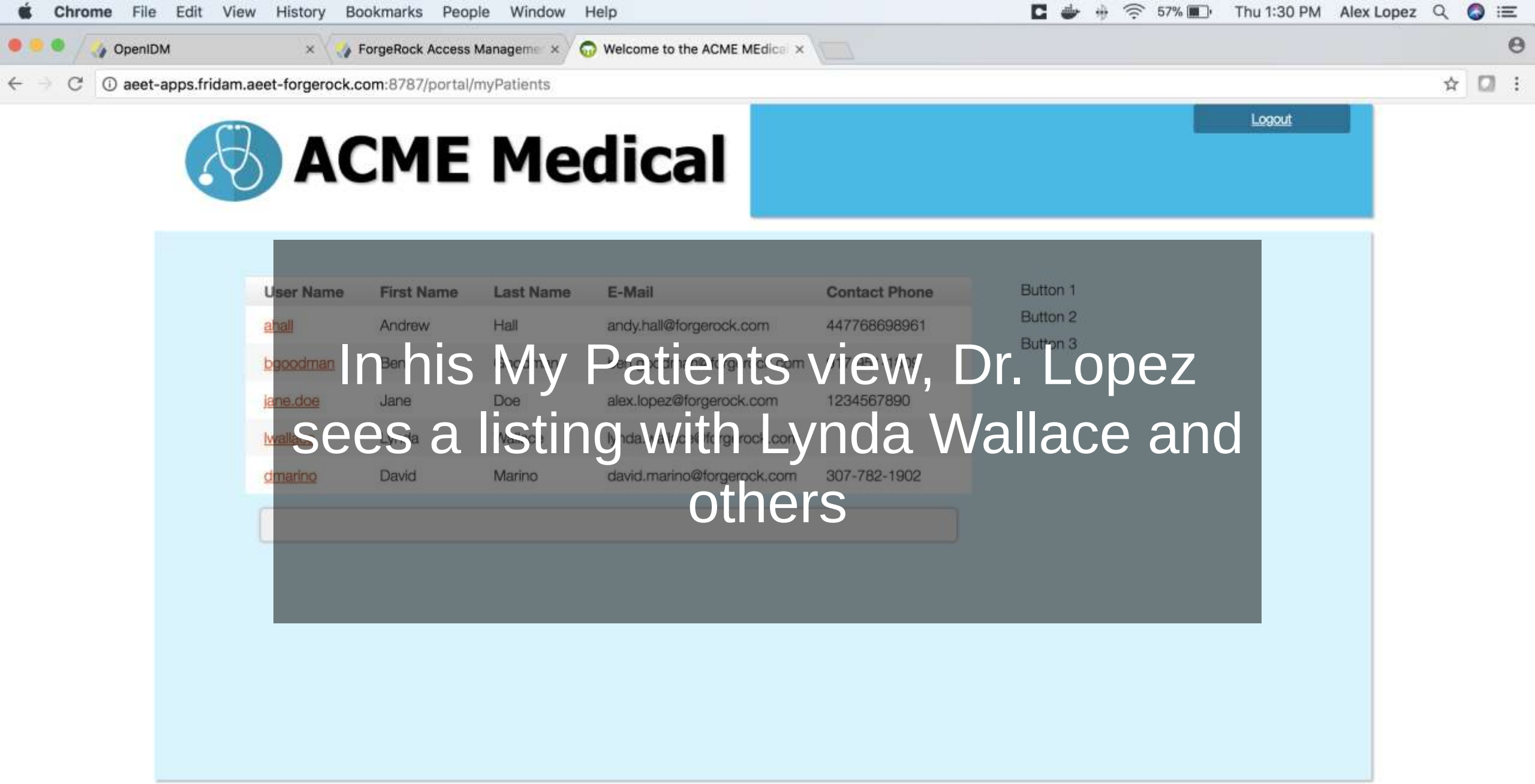
The mobile app securely mediates an oximeter data reading, and shows that the reading was successful

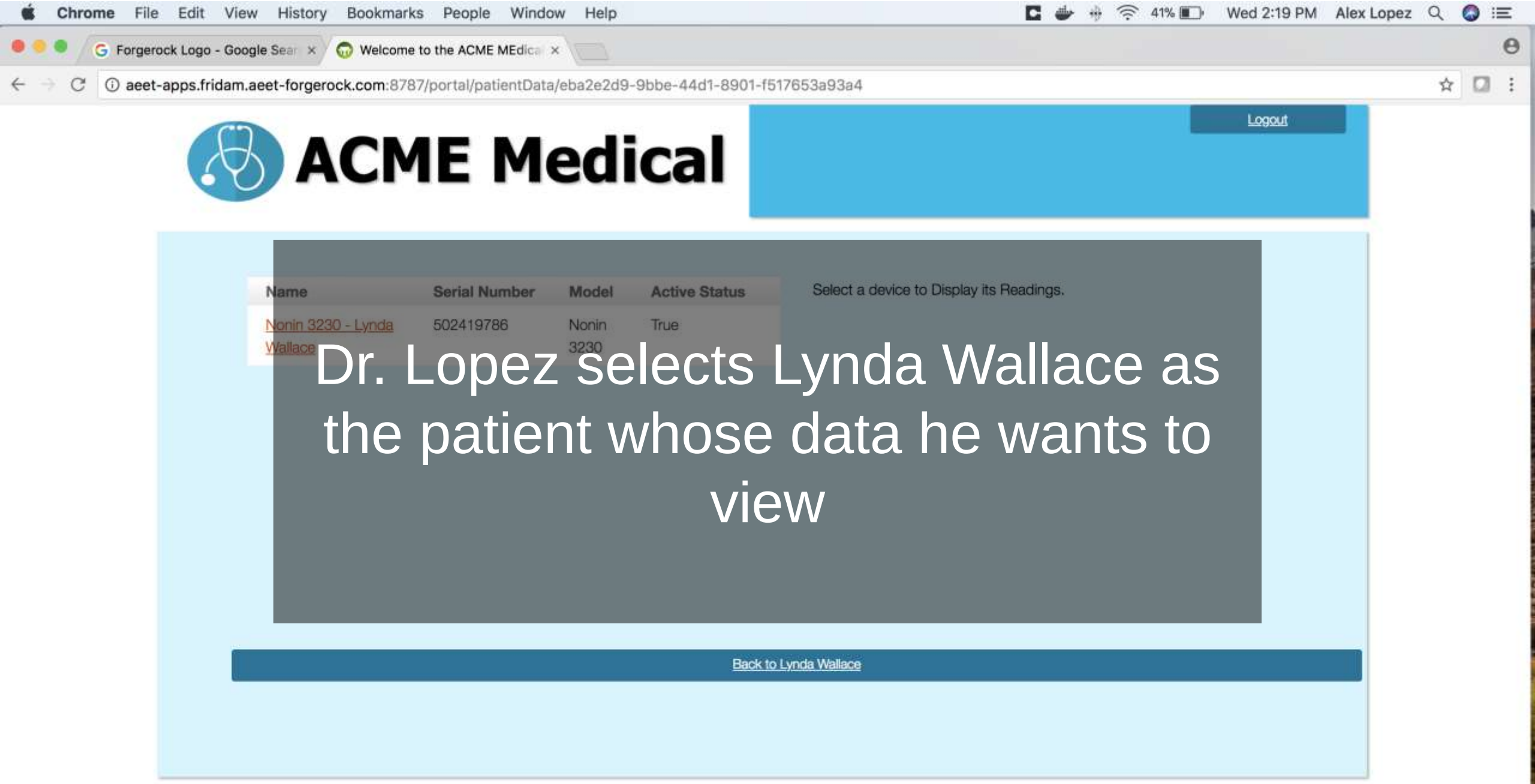


Dr. Lopez logs in to the ACME Medical portal



Dr. Lopez's view once authenticated is this home screen





Dr. Lopez selects Lynda Wallace as the patient whose data he wants to view

Chrome File Edit View History Bookmarks People Window Help 41% Wed 2:21 PM Alex Lopez

Forgerock Logo - Google Sear × | Welcome to the ACME Medical ×

aeet-apps.fridam.aeet-forgerock.com:8787/portal/showPatient/eba2e2d9-9bbe-44d1-8901-f517653a93a4

ACME Medical

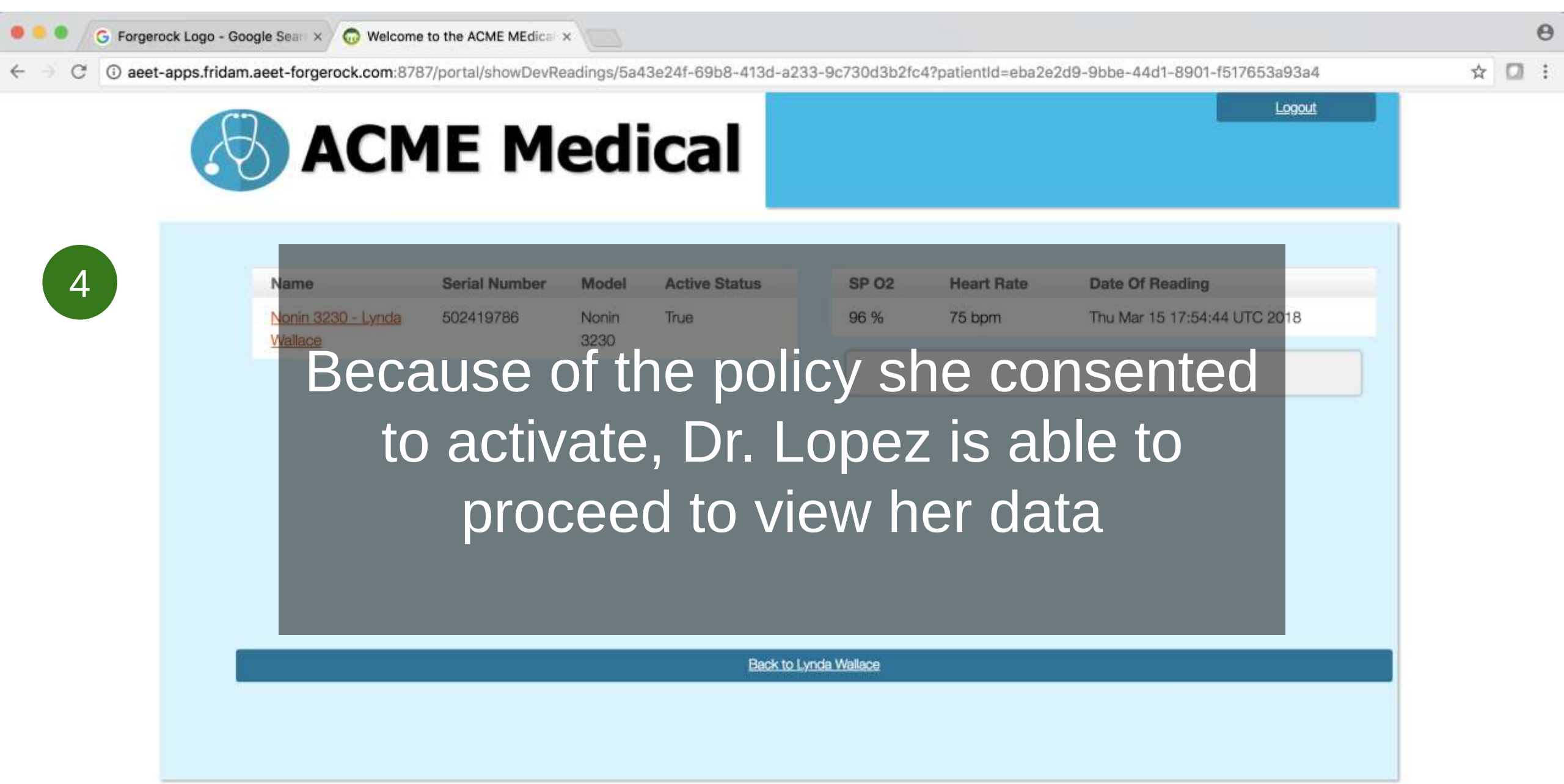
Logout

User Name	lwallace	Name	Nonin 3230 - Lynda Wallace
First Name	Lynda	Serial Number	502419786
Last Name	Wallace	Model	Nonin 3230
E-Mail	lynda.wallace@forgerock.com	Active Status	
Contact Pref			

He chooses Lynda's device profile

Back to Patients | Patient Data | Prescribe Device | Appointment History

aeet-apps.fridam.aeet-forgerock.com:8787/portal/patientData/eba2e2d9-9bbe-44d1-8901-f517653a93a4



4

Because of the policy she consented to activate, Dr. Lopez is able to proceed to view her data

5

The User-Managed Access (UMA) 2.0 grant of OAuth:

a) gives his client app a permission ticket on first resource attempt

b) requires an ID token for proof

c) issues an access token

d) requires it for data access

colin@kantarainitiative.eu

Twitter: @KantaraColin @KantaraNews

Join us at https://kantarainitiative.org/membership/

Newsletter sign-up:

https://kantarainitiative.org/reports-recommendations/