HEART Use Case – Alice electronically shares data from her PHR.

Description

Alice has a personal PHR that allows her to import her medical data from multiple sources. She can also enter her over the counter meds and other patient entered medical data. Alice would like to share that data with both physicians and/or family members.

Alice also has access to a trusted system where she can create electronic consents for her clinical data. This system utilizes identity assurance, so we know that Alice is who she says she is. This consent system also has access to an external trusted IdP, that includes a clinician profile with information about the physicians with which Alice wishes to share.

Alice creates an electronic consent, indicating that she wishes to share her medical record, from her PHR, with Dr. Erica, for a time period of 12 months. That's it for Alice, she has indicated her consent and she is done.

Meanwhile, Dr. Erica receives an email telling her that Alice has shared her medical record Alice's PHR. Dr. Erica uses her HEART client, which is like a SMART on FHIR app, with a little HEART added to it. Dr. Erica follows the link, she is asked to authenticate using her existing credentials (in the external trusted IdP) and she is provided with FHIR-based access to Alice's medical record. Since Alice has given her access over a 12-month period, Dr. Erica can access her medical record as needed and will have access to any updates made to her PHR.

HEART uses existing standards (HL7 FHIR, OAuth, OpenID Connect and UMA) to validate and authenticate Dr. Erica, then interpret Alice's electronic consent, to determine which parts of Alice's medical record are authorized to share with Dr. Erica. Using these standards and conforming to privacy and security best practices, only the authorized data is accessible to Dr. Erica. This system allows the data to flow while maintaining privacy, security, and Alice's sharing preferences.