HEART Use Case: Alice wants her spouse, Bob, to have access to her clinical records

Problem Statement

Alice has clinical data that she would like to share with her spouse Bob. The data resides in her health system's Patient Portal. She doesn't want to simply give Bob her personal login credentials but would rather provide him the means by which he could gain access using his own credentials. Also, she would like to be able to revoke his credentials at any time as she sees fit and she would like to be able to restrict his access to only certain elements of here clinical information (for example, to be able to view her medication list only).
Alice would like to manage this consent on her own and not have to go through Health System A's IT department to set this up.

Ecosystem parties

Alice is the patient
Bob is the spouse
Health System A is a health system where Alice has records. Health System A has a patient portal

Use Case

Situation:

Alice has records located in her Health System's Patient Portal and wishes to allow Bob access to her data that resides there

Because the PHI is under the control of a covered entity (the health system) it must meet the security and privacy requirements under HIPAA. As a result, only authorized individuals and their delegates can access the information within a patient's portal.

1) A health system would be unaware if Alice provided her login credentials to her spouse, Bob, unless they designed the login process in such a way as to prevent a non-authenticated user access to the account (for example, a design with strong MFA that supports authentication features that only Alice could provide (a facial biometric feature for example) or that continuously authenticated the user's identity throughout the online experience
2) The better design is support for the HEART protocol whereby Alice can establish revokable consents and allow another person (such as Bob) open or restricted access to her health system's patient portal.

In both situations listed above, the most secure and privacy enhancing design is enabled via HEART protocol whereby Alice can easily establish and manage her personal consent policies.

The Consent Policy Management process would have the following characteristics:

- Strong Authentication whereby only Alice could gain access to the consent policy management screens
- A UI and workflow that is easy for a typical patient/consumer to use
- Ability to add or select the individual to whom the consent applies
    - Adding a new individual would necessitate some key details:
        - Person's name
        - Person's contact information (email address)
    - Selecting the individual (a healthcare provider) from a pre-established list:
        - An updated, confirmed list of healthcare providers with sufficient details to help the end-user search, filter and select the right individual (Provider Directory)
- Ability to provide some level of granular consent (share all, share only certain details, share only under certain circumstances)
- Ability to provide a start and stop consent date
- Ability to revoke a consent

Once a consent policy is created, the recipient of the consent (Bob) should provide electronic confirmation that they have received the request and agree to the terms of the consent. (via confirmation email or text message for this select purpose)

Alice should be made aware that the consent was sent, received/read, and either confirmed or declined by Bob.

Alice should be able to view all individuals who have a consent (either currently active, previously active) and manage their status (revoke, re-activate, update details)

Situation 3. Bob's Role

As the receiver of the consent, Bob also has a role to play in this use case.

1) Bob needs to be able to electronically receive the consent invitation from Alice
2) Bob needs to be able to review any terms of the consent and electronically agree to or decline the invitation
3) If Bob agrees to the consent then he will be provided a link whereby he can electronically gain secure access to the location where Alice's records are maintained (PHR or Patient Portal).
4) It is from this link that Bob will be able to login and view, print and possibly download and transmit Alice's clinical data.