MVP Patient Consent Data Model Changes

⚠ **Status**: DRAFT

Background

Patient data is valuable both for patient care and for research purposes. However, access to that data should be in accordance with the wishes of the patient. This proposal suggests an all-or-nothing approach to granting read access to patient data.

Overview

Access to patient data should be restricted to authorized parties in accordance with the wishes of the patient or their legal representative.

Use Case - Data Capture

While the initial recording of patient data requires temporary knowledge of that data, it does not imply patient consent for authorizing future reading. The contribution of data should be decoupled from access to data – as far as practically achievable, it is a write-only operation.

Goal: allow restricted access to data during capture

Steps:

1. Present input interface
2. Accepts input data
3. Temporarily store data
4. Store data in permanent, secure storage
5. Remove data in temporary storage

Use Case - Authorize Access to Patient Data

All patient data is by default inaccessible to all parties. Explicit consent is required to gain read access to patient data.

Goal: to explicitly authorize access to patient data

Steps:

1. System presents authorization interface to user
2. User explicitly indicates authorized parties
3. System records authorization of patient data

Notes:

- authorized parties - any legal entity, whether an actual individual, members of a group or an organization

Use Case - Consensual Data Export

Data export routines should respect the authorization constraints on patient data, filtering out data which has not been explicitly marked as available to the export consumer.

Goal: only export data which has been explicitly marked with patient consent

Steps:

1. Select only patient data which has been explicitly marked
2. Export the data

Design Proposal

Interested Parties

?Unknown User (akanter)