Embleema FHIR App Development Guidelines Summary

Version: September 2019
Last Edit: November 2019

At Embleema, we strive to be good data stewards to maintain our users' trust and make the healthcare ecosystem more efficient. This document details some of voluntary features and processes that we have adopted to improve data privacy, security and accuracy, in line with the ONC Certification requirements. This public documentation details the equivalent functionality we developed, in lieu of formal certification.

With the lack of a unified source of medical data, tests are repeated, the same questions are asked at visits and outdated information is associated with our medical files. By empowering users to control their data, they can see all of their health and wellness data in one spot. Patients can use the Embleema website and apps free of charge.

45 CFR 170.315 (b)(6) (Data Export):
We're deep believers in data portability and we strive to adopt the latest HL7 standard. As a result, users have the option to export their data. They can also select specific data types, healthcare locations and time periods for the extract. Export summaries can be available in a C-CDA compliant format. In case a user has access to records from several individuals, the data can be grouped into a unique export if needed. When available, data is exported using public coded data vocabularies and ontologies.

45 CFR 170.315 (d)(1) (Authentication, Access Control, Authorization):
Users are assigned a unique ID and asymmetric key pair. All users are authenticated with email / passwords and 2FA authentication can be available as an option. All data access permissions are recorded and maintained in relation to the user's public key. Each time a user requests access to a data element, access rights are checked and validated against his/her key.

45 CFR 170.315 (d)(2) (Auditable Events and Tamper-resistance):
Any change to a user data is tracked, recorded and versioned. Our metadata notably includes user ID, date and time.

Any changes in user privileges is immutably tracked with the associated user ID, date, time and scope of the new privilege.
If encryption status of locally stored data on an end-user device is changed, we record the user ID, date, time and scope of the change.
All audit logs are stored in a data warehouse where modifications are not allowed.

45 CFR 170.315 (d)(3) (Audit Report(s)):
We support the generation of audit reports. All reports are sortable and include data, time and the categories of the corresponding actions.

While this is not included in the scope of 45 CFR 170.315 (d)(3), *we also allow patients to directly audit the access logs corresponding to their data as well as track any modification to their medical records.*

45 CFR 170.315 (d)(5) (Automatic Access Time-out)
If inactive for a certain period of time, users are logged out of our system. They need to re-authenticate to access their data again.

45 CFR 170.315 (d)(7) (End-user Device Encryption):
We perform at-rest encryption if data is stored on an end-user device.

45 CFR 170.315 (d)(8) (Integrity):
A hash is always associated with any health data to allow for integrity protection and allow the detection of any potential improper modifications. Our computational pipelines are also tracked through their hash value for the same reasons. Hash are created with SHA-2 algorithms.

45 CFR 170.315 (d)(9) (Trusted Connection):
All users connections are done using https. We only use TLS 1.2 or above cypher suites.

45 CFR 170.315 (d)(11) (Accounting of Disclosures):
Not applicable. Based on the scope and use cases of our product today, don't need to disclose any information for treatment, payment, and health care operations.

45 CFR 170.315 (g)(3) (Safety-enhanced Design): "User-centered design processes must be applied to each capability technology."

Users are aware that this tool is aggregating health data for personal use but can also opt to share their data to specific users or for clinical research.

Users are made aware of where their information is stored, that it is not tampered with and can specify each section when opting to share any data in a clearly labelled and guided process. There are multiple ways of accessing their health data sharing page and all entities with access are listed and each section where they have access clearly labelled.

The process of connecting data is clear and guided, with help always available, including contacting us directly. Users are also made aware that they can opt out at any time.

45 CFR 170.315 (g)(4) (Quality Management System):
We have a documented System Development Lifecycle. Our QMS notably ensures that we apply appropriate risk management
strategies, good design practices, adequate verification and validation, and appropriate methods to correct and prevent risks to our users.

45 CFR 170.315 (g)(5) (Accessibility-centered Design):

Our design has taken into account contrast with text (4:85:1) and icons, the use of clear labelling alongside iconography and color vision deficiency awareness by the use of clear labelling alongside color indicators. All available action buttons are clearly marked with a rollover state.

Users have clear ways to reach out for help or get guided through processes. Tooltips are utilized where we felt any potential clarification would be helpful. Error messaging is clear and specific and when no data is present, the section is clearly marked as empty.

The design has been tested by users varying in age, eyesight, technical ability and preferred device. Text is basic and conversational for users to understand each step.

45 CFR 170.315 (g)(7) (Application Access - Patient Selection):
After a patient grant data access and after successful patient identification, a unique ID is shared with the 3rd-party application. This will be used to subsequently retrieve data. Registration of 3rd-party applications is necessary and only secured encrypted communications are allowed.

45 CFR 170.315 (g)(8) (Application Access - Data Category Request):
Data can be queried by categories, based on the FHIR 4.0.1 ressources. All available data categories from the Common Clinical Data Set are accessible. Request can contain a specific data or date range. All data for the category are returned in a FHIR-compliant format.

45 CFR 170.315 (g)(9) (Application Access - All Data Request):
Upon user's action, all of the data categories specified in the Common Clinical Data Set can be retrieved at one time in a summary record formatted according to the Continuity of Care Document (CCD) template.

45 CFR 170.523 (k)(1) (Pricing Transparency):
See introduction paragraph for disclosure of end-user pricing.

45 CFR 170.523 (n) (Complaint Process):
We can share a list of complaints received to the National Coordinator on a quarterly basis each calendar year that includes the number of complaints received, the nature/substance of each complaint, and the type of complainant for each complaint.