2020 Innovator Fellowship Program

Patient Access API: The Current State of Consent and Opportunities for Innovation

"A record of a consent transaction enhances the ability to maintain and manage permissions for personal data by both the individual and the organization [1]."

Background and How We Got Here

On April 21, 2020, the Centers for Medicare & Medicaid Services (CMS) issued a final rule (CMS-9115-F) on interoperability that requires payers to expose patient's health care data they hold through Fast Interoperability Healthcare Resources (FHIR) based application programming interfaces (APIs) [2]. One of the primary goals of the rule is to allow patients to have access to payer's data (e.g., clinical data, claims) via any 3rd party application (apps) of their choice. The rule will be effective starting on January 1, 2021, with discretionary enforcement moved out to July 1, 2021. The rule reflects CMS' goal to put the patient at the center of health care and facilitate "liberating patient data" so patients can better manage their healthcare and see the associated costs [3]. Many patients are very supportive of this move. A recent PEW survey conducted with 1,213 adults between June 1 and July 3, 2020 indicated that 61% want access to their medical information to manage their own health [4]. The rule is also aligned with the HIPAA individual right to access that dictates that patient's have a fundamental right for access to their protected health information (PHI) [5].

By implementing this new rule, not only are patients now at the forefront of health care interoperability, but also the 3rd party apps that they will be using to access their data. Many of these health based apps can provide consumers with valuable insights, offer a holistic view of their health, and promote continuous care. However, during the open public comment period for the rule, CMS heard many concerns about security and privacy of patients data and their use of mobile health apps. As a result, CMS added an educational component in the rule so that payers can help patients to understand what they are consenting to when allowing an app to access their health care data [6]. Also, patients need to understand the fact that once their data leaves possession of the payer, the data is no longer protected by the strict privacy and security standards covered by the Health Insurance Portability and Accountability Act (HIPAA). However there are other rules the data are subject to when in possession of the app, which are governed by the Federal Trade Commission (FTC)[7]. There is some hesitation from patients in providing their data to apps under certain circumstances, for example, 56% of the patients from the PEW survey indicated they are not comfortable sharing their data with apps that are not pre-approved by an oversight body or independent certification boards [8].

Patient Access API Consent Requirements - Current State

For years, consent has been critical in protecting against unauthorized inappropriate use of patient data and ensuring it is protected. While crucial for patient privacy, consent has also proved to be a challenge and at times a barrier for interoperability across the Cambia Grove 5 Points of Healthcare™ (Patients, Providers, Payers, Policymakers and Purchasers)[9]. To reduce administrative burden, and allow patients frictionless access to their health care data, CMS and the Office of National Coordinator (ONC) came to agreement that payers should use well-vetted FHIR profiles to support app registration and authentication. The CMS rule requires payers to implement the Substitutable Medical Applications Reusable Technologies (SMART) Application Launch Implementation Guide and the ONC 21st Century Cures Act requirement that they support "SMART on FHIR Core Capabilities" [10]. SMART on FHIR [11] is built off of the long established OAuth 2.0 and OpenIDConnect protocols used in app launch, authorization and registration processes across many industries outside of healthcare.

In general, these are the processes that payers either are required to or should implement related to allowing access to patient data to 3rd party apps and ensuring their patients understand what they are authorizing in terms of the API:

1. Registration
2. Authorization
3. Attestation (optional)
4. Education

Registration: For an app to register with payers, apps should use the OAuth 2.0 Dynamic Client Registration Protocol [12] or a manual pre-registration portal at the authorization server that issues an initial access token. After registration, the application is launched, the launch context determines available scopes which represent allowable data boundaries for application.

Authorization: For apps to be authorized to access patient data that a payer holds, apps will need to do so using the OpenIDConnect (OAuth 2.0 & OpenID) protocols including exchange of id, client secrets, security tokens [13] and access tokens.

Once an app has properly registered and authorized by end user (patient), the app is able to access any data the payer holds outlined in the CMS rule, including claims and clinical data

Attestation: An optional step that payers can implement is an attestation process in which apps are asked to attest to certain privacy, security and data usage standards. CMS suggests payers use industry the CARIN Alliance's Code of Conduct and the ONC Model Privacy Notice and other industry best practices for other items they can include in their attestation process [14][15]. However, apps are not required to respond to the attestations, and in that case, payers can notify their patients that the app they have chosen to share their data with did not attest to certain privacy conditions.

Education: Patient education is a requirement under the final rule where documentation and communication of how their health data is being used, should be provided in a simple context. The challenge we bring forward is how can payers educate their members on what a covered entity is, given the fact that once the payer releases their data to a third party app, their data is no longer protected by HIPAA, if the app is produced by a non-covered entity. Creating educational communications around technical solutions is always a difficult task, but payers will need to do what they can to ensure their patients understand the protections that exist for their data once it leaves the payers possession.

Currently in the Patient Access API rule, the consent for access to the patient's data to a 3rd party app under the rule is all or nothing. There is no requirement to allow a patient to have more granular control of consent over their data.

Project goal

Our project research focused on user level consent and patients sharing their healthcare data with third party apps as it relates to the Patient Access API rule, but our intent is not at all to question whether the rule goes far enough in terms of consent, as the rule directs payers to use highly effective and mature security and authentication protocols (OAuth 2.0, OpenIDConnect and SMART on FHIR). We see this as a potential opportunity in advancement in the future, to allow more granular control for patients when it comes to the health care data that they provide access to the apps. Ultimately our goal with this project was to highlight some of the challenges that exist around granular consent, some of the solutions that other industries, such as the financial sector have implemented, and to acknowledge some of the current health care and FHIR-based consent and identity resolution sponsored projects currently in-flight.

Our Approach to this Work

In order to obtain information and insights of the Patient Access API and consent, these are the activities we undertook to best inform our learnings and potential future solutions:

- Conducted interviews across the 5 Points of Health Care™, and those experts in consent, interoperability and FHIR.Through these interviews we gained invaluable insights, perspectives and opinions on the Patient Access API and specifically consent, including any challenges and the future opportunities around patient privacy and security
- Conducted an informal patient survey to understand the expectations and perspectives from patients on their data privacy
- Researched solutions from other industries on how they handle consent and data sharing
- Researched current efforts and project underway in health care and specifically FHIR-based consent and identity resolution use cases

We used all of these sources to draw from for our work and what formed our findings and conclusions around consent for patients accessing their healthcare data.

Our Findings: Challenges and Current Efforts on Granular Consent

Challenges: In the current state of granular consent there are challenges to overcome, mostly technical in nature and the current state of the standards being used. Also, in terms of the Patient Access API, ONC acknowledged the following in the final Cures Act rule [16]:

"At this time, FHIR Release 4 version of FHIR consent resource is not normative and can change from version to version and therefore further development, review, balloting, and testing would be required for a FHIR Release 4 based IG to be a viable consensus standard for adoption in the Program. In consideration of comments, and the scope of the additional work required for readiness of an IG that could be adopted in our regulations, *we have not finalized the proposed "consent management for APIs" certification criterion in § 170.315(g)(11). "*

In addition to further maturity of the FHIR Consent resource, most current consent solutions are a contrast between either "all or nothing" or being too overly granular the user is overwhelmed and confused. When done poorly, granular consent increases the cognitive burden on the user/patient. One challenge is the interface (UI/UX) imposed cognitive burden for the patient when it comes to consent and their ability to comprehend, much less fine tune, what they are being asked to consent to. The second challenge is the implementation of granular consent, and how you can represent granular controls using FHIR's Consent resource. A third challenge is specific to SMART on FHIR specification only has resource level scopes, not at an attribute level, so if an app is granted access to the Observation resource it has access to all of the Observation resources for a patient. Another difficulty is around consent revocation using the FHIR Consent resource, and how to make that work properly. Finally, provisioning access to health care data for a patient's authorized representative, caretaker, or parent is another difficult use case that will need to be solved related to consent.

Patient Survey: To get our own sense of how patients feel regarding control over their healthcare data we conducted a survey of patients to see how they felt regarding control of their health care data. Our survey was conducted with 73 patients and it showed:

- 95% of respondents indicated the importance for them to have authority to manage what health care information a third party app can access.
- 66% responded that it's important for the payers to monitor or be aware of what the third party app wants to do with the patient data health data
- 98.7% would like to be presented with a list of their health information that they can select and approve the health app to access

Our results, while with a very small sample size, show that patients find it important to feel in control of their data and prefer to have a granular approach to consent where they can select and approve what information the apps can access.

Our interviews with stakeholders have helped confirm the findings of the patient survey. Based on this information, we foresee the need for patients to eventually have more granular control of their health care data, not in an effort to make interoperability more difficult, but rather, continue to empower patients to determine who can access their data, what can be accessed, and for what purpose. As FHIR resources, profiles and implementation guides continue to mature, we see the opportunity for the allowance of granular controls of their health care data.

Our findings are aligned with what we have found from other industries in the advancements they have made to help their clients manage data sharing with the 3rd party apps. For example, in banking and financing, 80% percent of clients do not realize that the 3rd party may store their bank account and passwords and about 79% don't read the terms and conditions of the apps [17]. To give their customers more transparency into who holds their financial data, some banks have developed dashboards in which the clients can see which apps their financial data has been shared with, and allow customers to revoke access if desired, the Wells Fargo Control Tower is just one of many that exist [18]. When it comes to the Patient Access API, much like a bank, a payer has the visibility to all of the apps that their patients have allowed to access their health care data. As a result of this holistic, longitudinal view of who has access to their data, payers can develop similar solutions to allow patients the ability to know who has access and allow them to revoke that access.

Parallel efforts in the area of decentralized identity can provide an ideal starting point for better consent management. To achieve a decentralized identity, a trust framework needs to be created around these decentralized identity providers. While the focus of our project was not digital identity management or trust frameworks, we feel advancements in these areas are foundational precursors to better consent management. We want to highlight just a few of the current FHIR based efforts underway related to consent and digital identity management. This is by no means an exhaustive list, but some that we looked into that we wanted to highlight as efforts to take consent and identity management to the next level:

- Kantara Initiative [19]
    - Kantara introduces the concept of a "consent receipt" and their specification defines the requirements for a record of a consent interaction (or consent record summary linked to the record of consent provided by a personally identifiable information (PII) Principal to a PII Controller (e.g. apps) to collect, use and disclose the PII Principal's PII in accordance with an agreed set of terms. The terms and conditions are then stored in the consent receipt [20]. There are two representations of the consent receipt stored with this framework, one human readable and one machine readable.
    - Kantara also has an identity assurance and trust framework as well to advance capabilities around digital identity.
- Unified Data Access Profiles (UDAP) - EMR Direct [21]

    - Unified Data Access Profiles (UDAP) can increase confidence in open API transactions through the use of trusted identities and verified attributes
    - UDAP is a foundational component of the ONC FAST Security Tiger Team Solution [22]
- Consent2Share [23]:
    - Developed by the US Substance Abuse and Mental Health Administration to support behavioral health data integration with FHIR Servers, including substance use and mental health data.
    - Consent2Share brings forth the standards set in the Data Segmentation for Privacy (DS4P), which is sponsored by the ONC to help better protect the sensitive data for patients receiving behavioral health treatment.
- SMART 2.0 (CRUDS - granular controls) This is an active Argonaut project that aims to provide [24]:
    - improved SMART App Launch Framework, including token introspection and finer-grained access controls for patients, allowing them to be specific about what portions of their health care data that apps can access
    - more detailed constraints based on small common core of FHIR REST API search parameters e.g. _tag, _security, category
    - detailed suffixes to convey support for create, read, update, delete and search interactions with FHIR REST API e.g. write interactions are represented as .cud
- ONC Privacy and Security Framework for Patient Centered Outcomes Research (PCOR)
    - Developed “granular choice” use cases and proposed several FHIR-based standards that could be used in order to meet the requirements of those use cases [25]
    - Published use case white paper in July 2020, FHIR resources proposed for use were:
    - FHIR Questionnaire Resource [26] and FHIR Questionnaire Response Resource [27] for an electronic consent form
    - FHIR Consent Resource [28] for encoded reports about a consent directive, and for encoded legally binding consent directive
- Federated Identity Management (CARIN Alliance) [29]:
    - CARIN Alliance is supporting multiple efforts around federated identity management, “..to digitally identify individuals across systems without the need for portals” [30]
    - CARIN produced a “CARIN ID Proofing White Paper” that takes a detailed and deep-dive into why ID proofing is important to health care organizations and in accordance with NIST guidelines [31]

Where We Go From Here

Over the next few years, as the interoperability rules are implemented by payers and providers, there will be a retrospective done to see what more can be done related to consent, not only from a technology and data perspective but also through policymaking. As you can see, there are many efforts already in-flight looking to implement standards-based approaches to help the industry handle granular consent. These various initiatives, Standard Development Organizations, and regulatory bodies are working towards this goal, which will benefit patients, while at the same time, not negatively impacting interoperability by introducing friction. Through advancements in our standards, frameworks and implementation guides, granular consent can play a critical role in expansion of interoperability across the entire health care spectrum. Other industries have solved for this, and with the projects we have highlighted here - there is plenty to be optimistic about for health care in the very near future.

Cambia Grove Innovator Fellowship Authors:

Doan Ha - Performance Improvement Director, Cedar Hills Hospital

E-mail: doanha82@gmail.com

Phung Matthews- PharmD, FACA, Consultant, Point of Care Partners (PCOP)

E-mail:Phung.Matthews@utah.edu

Aju Jacob - Enterprise Architect, Blue Cross Blue Shield of Tennessee
E-mail: aju_jacob@bcbst.com
LinkedIn: https://linkedin.com/in/ajujacob

Daya Sharma - CTO, The Handoff Company
E-mail: daya@caringly.io
LinkedIn: https://linkedin.com/in/dayas

Mike Barabe - Enterprise Data Architect, Washington State Health Care Authority
E-mail: michael.barabe@hca.wa.gov
LinkedIn: https://www.linkedin.com/in/michael-barabe-059a215b

Citations

1. **Kantara Consent Receipt Specification:** File Download: Consent Receipt Specification – Kantara Initiative
2. **CMS Final Interoperability Rule:** CMS Final Interoperability Rule
3. **CMS Interoperability Site:** CMS Interoperability and Patient Access final rule
4. **PEW Health Care data survey:** Americans Want Federal Government to Make Sharing Electronic Health Data Easier
5. **Combined HIPAA Rule:** https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf?language=es
6. **CMS Final Interoperability Rule:** CMS Final Interoperability Rule
7. **Healthcare Financial Management Association - Summary of Final Rule, Page 4:** CMS Interoperability Patient Access to Health Data Final Rule Summary
8. **PEW Health Care data survey:** Americans Want Federal Government to Make Sharing Electronic Health Data Easier
9. **Cambia Grove:** 5 Points of Health Care
10. **21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program:** Federal Register/Vol. 85, No. 85/Friday, May 1, 2020/Rules and Regulations
11. **SMART:** https://docs.smarthealthit.org/
12. **OAuth 2.0:** https://oauth.net/2/
13. **OpenIDConnect:** https://openid.net/connect/
14. **CARIN Alliance:** Trust Framework and Code of Conduct

15. **ONC Privacy Model Notice:** Model Privacy Notice (MPN) | HealthIT.gov
16. **21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program:** Federal Register/Vol. 85, No. 85/Friday, May 1, 2020/Rules and Regulations
17. **The Clearing House: "**Consumer Survey: Financial Apps and Data Privacy**", November 2019**
18. **Wells Fargo Control Tower:** https://www.wellsfargo.com/online-banking/manage-accounts/control-tower/
19. **Kantara Initiative:** https://kantarainitiative.org/
20. **Kantara Consent Receipt Specification:** File Download: Consent Receipt Specification – Kantara Initiative
21. **UDAP:** https://www.udap.org/
22. **ONC Privacy & Security Tiger Team:** https://oncprojectracking.healthit.gov/wiki/display/TechLabSC/Security+Tiger+Team
23. **Consent2Share:** consent2share/README.md at master · bhits/consent2share · GitHub
24. **SMART v2.0 CRUDS:** https://github.com/HL7/smart-app-launch/blob/master/fsh/ig-data/input/pages/scopes-v2-wip.md
25. **Argonaut Project (Granular Consent):** Argonaut Current Projects - HL7 Argonaut Project Wiki
26. **HL7 Questionnaire Resource:** http://hl7.org/fhir/questionnaire.html
27. **HL7 Questionnaire Response Resource:** http://hl7.org/fhir/questionnaireresponse.html
28. **HL7 Consent Resource:** http://hl7.org/fhir/consent.html
29. **ONC PCOR Enabling Granular Choice:** Enabling Granular Choice for Health Care Delivery and Research Consent
30. **CARIN Alliance Consumer ID and Authentication:** Consumer ID & Authentication
31. **CARIN ID Proofing White Paper:** Patient Identity Proofing