Consent Tracker FHIR Resource Proposal

Consent Tracker

Owning committee name
Community-Based Collaborative Care

Committee Approval Date:
May 31, 2016
Approved during the May 31, 2016 CBCC Conference Call

Contributing or Reviewing Work Groups
- Security

FHIR Resource Development Project Insight ID
pending - reminder sent to CBCC cochairs June 1, 2016

Scope of coverage

Consent Tracker Scope of Coverage
- Important decisions that patients and their personal representative make about activities or information, which concern their health and well-being, are typically captured as contractually binding permissions, obligations, and prohibitions known as Consent Directives. Consent Directives memorialize these decisions as rules specifying rights that the patient, as grantor, conveys to a grantee, such as a provider, a health app, a health plan, HIE, or clinical trial.
- When patients and providers create and manage privacy and medical Consent Directives, including clinical trial, research, and advanced directives, three components are typically required:
1. Paper or electronic forms in which a patient documents permissions granted or restriction limiting activities related to e.g.: patient care [aka medical consent directive], participation in clinical trials [aka research consent directive], or collection, access, use, and disclosure of information [aka privacy consent directive]
2. The legally binding recording of a Consent Directive contract for which both the patient grantor and the data controller or processor grantee are held accountable once executed. A legally binding Consent Directive may transition a series of lifecycle stages or 'statuses', which may indicate e.g., whether the Consent Directive form has been signed by the patient and accepted by the grantee, whether the patient has revoked or renewed it.
3. A means for managing or "tracking" Consent Directives at all stages in their lifecycle, from the patient, institutional, or jurisdictional policy, to an offered Consent Directive form, and on to the executed Consent Directive, which may be pending, disputed, revoked, terminated, or renewed.

- The FHIR Consent Tracker Resource supports the third requirement by providing a flexible means for tracking and conveying intra-and inter-enterprise the lifecycle, provenance, privacy, and security metadata used for Consent Directive management workflows, such as obtaining patient authorizations and restrictions, and Consent Directive enforcement using security labeling and privacy protective services to comply with access control decisions.
- The Consent Tracker Resource is agnostic to the media used to capture the Consent Directive. I.e., it can track the location from which an authorized user may retrieve a copy of or verification of the existence of a legally binding Consent Directive regardless of whether it is captured as a paper, scanned or otherwise unstructured representation; IHE Basic and Advanced Patient Privacy Consents; HL7 CDA Consent Directives, a FHIR Consent Directives, or the patient friendly FHIR Consent Directive form and completed instance, i.e., a FHIR Consent Directive Questionnaire and Questionnaire Response.

Evidence of utility for 80% of Systems

- The proposed Consent Tracker Resource is intended to meet a very basic yet unique healthcare domain business requirement, which is to convey the minimal set of consent directive metadata that has been used by the industry to manage consent directive in various workflows, such as orders, observations, ADT, claims, and records management and lifecycle status notifications; and access control use cases related to those workflows including collection, access, use, and disclosures of the consent directive metadata and access restriction parameters (e.g., location, user department, caregiver-patient relationships, other access restriction parameters) to determine user access.
- The Consent Tracker Resource elements were selected based on mapping several current approaches to conveying consent directive metadata.
- V2 approach to managing consent directive metadata includes sending the metadata in a CON segment and/or populating elements in other message types:
  - v2 CON Medical Records Consent Segment: This segment identifies patient consent information relating to a particular message. It can be used as part of existing messaging messages to convey information about patient consent, authorizations and restrictions, and Consent Directive enforcement using security labeling and privacy protective services to comply with access control decisions.
  - CON Segment elements include consent type, form id and version, recorded consent unique identifier (whether on paper or electronic), access restriction parameters, status, consent recorded and effective date/time, bypass and non-disclosure reason (v3 purpose of use and sensitivity code such as taboo)
  - CON segment may be used in MDM/ACK - Document Status Change Notification (Event T03), Document Status Change Notification and Content (Event T04), Document Addendum Notification (Event T05), Document Addendum Notification and Content (Event T06), Document Addendum Notification (Event T07), Document Edit Notification and Content (Event T08), Document Replacement Notification (Event T09), Document Replacement Notification and Content (Event T10), Document Cancel Notification (Event T11)
  - v2 MDM/ACK - Document Status Change Notification (Event T03): This is a notification of a change in a status of a document without the accompanying content. Scenario: A document is authenticated. Notification is sent to the chart tracking system and is used to update the document status from pre-authenticated to authenticated or legally authenticated. A change in any of the following independent status characteristics would cause a message to be sent: Completion Status and Confidentiality Status.
  - An ARV-3 Access Restriction Value: The ARV segment is used to communicate the requested/required type of access restrictions from system to system, at both the person/patient and the encounter/visit level
  - Examples: A person/patient may have the right to object to any or all of his/her information to be disclosed. In addition, the patient may request that protected information not be disclosed to family members or friends who may be involved in their care or for notification purposes.
  - A realm or organization may have certain privacy policies. A patient may have the right to opt out of being included on facility directories. In an international context, a physician may be culturally obligated to protect the patient's privacy. Any "opt-in" or "opt-out" restrictions.
  - The individual system security may want to utilize the Access Restriction Value along with the Access Restriction Reason (and/or with the Confidentiality Code from another segment, e.g., OM1-30 or other data) in order to implement the appropriate type of protection for the person, patient, visit and/or visit data. Each system has the flexibility to incorporate/map the access values into their security system appropriately; the actual implementation for access to protected data is determined by the individual system. The Access Restriction Values supported by an enterprise/system would be defined and determined by that organization.
  - It is expected that these access restriction values would be utilized in combination with other system security information (e.g., patient locations, user department, caregiver-patient relationships, other access restriction parameters) to determine user access. System implementers should carefully control access to the restriction codes and values, as they themselves hold sensitive information.
  - OM 1-30 Master Files General Observations Confidentiality Code: This field contains the degree to which special confidentiality protection should be applied to the observation.
  - ORC-28 Common Order Segment Confidentiality Code: This field contains information about the level of security and/or sensitivity surrounding the order (e.g., highly sensitive, not sensitive, sensitive, etc.).
  - Financial Management DG1-18 Confidential Indicator and DRG-10 Confidential Indicator: Fields indicating whether the diagnosis is confidential or the DRG contains a confidential diagnosis.
  - eClaims EHC^E12 – Request Additional Information (event E12): Interpretative Rule: Patient Consent. If Patient Consent in the RFI segment is marked "Y" (Yes) the Payer is signifying possession of proof of patient consent for release of confidential information.
  - EHC^E13 – Additional Information Response (event E13): Informative Rule: Document Confidentiality Status on TXA. When this optional field is completed it indicates that the Payer is to restrict access to the attached document according to the Payer's established policies and/or in accordance with prior business agreements between the Provider and Payer.

Referenced, supported, supported by, or foundational v3 Privacy and Security specifications

- v3 Foundation Privacy and Security - all specifications including:
  - Security and Privacy Ontology - Ontological representation of all Privacy and Security vocabulary used in HL7.
• Privacy, Access and Security Services [PASS] Security Labeling Service, Access Control, and Audit Services Conceptual Models
• HL7 Role-based Access Control Catalog
• HL7 Healthcare Access Control Catalog
• HL7 Patient Friendly language for Security and Privacy for Consent Directives
• HL7 Privacy Impact Assessment Cookbook
• HL7 Privacy and Security Architecture Framework Project 914 - under development as an update to the HL7 Security and Privacy Domain Analysis Model

• CDA Consent Directive Implementation Guide
• CDA Data Segmentation for Privacy Content, Exchange, and Directive Implementation Guides
• CDA Data Provenance Implementation Guide

• v3 Medical Records Domain Data Consent Topic RCMR_ST010007UV Consent Manager: RCMR_AR010003UV and Data Consent Tracker: RCMR_AR010002UV:

• Privacy and Security Prerequisites for Document Queries: There are a number of privacy and security considerations the reader or implementer of document query messaging should consider in any given implementation use case for support of cross enterprise, cross application document queries. These concerns are especially important to help guard against unauthorized re-disclosure of information, and help build confidence that patient privacy and confidentiality can be upheld. These concerns include how evidence of a requestor's authorization may be provided or made available to provide validation to the recipient of the request that the requestor is making a valid request for release of information, how the recipient of the request has an appropriate level of trust (contractually, technically or legally) with the requestor and how patient rights to know of disclosures of personal health information may be enabled through auditing of such disclosures. There may be additional functional requirements and implementation requirements at the realm level.

• The prerequisites for privacy and security interests to be appropriately served in document query transactions are as follows:
  • Security context/Trust relationship exists between participants for each communication instance: These prerequisites outline the security requirements that should be in place to assure the trust relationship exists, and that the communication is done in a secure manner. They include: [1] Support for the confidentiality and integrity of the message itself through the use of appropriate security measures (e.g. encryption) [2] That the transmission is done in a secure manner [3] That the sender and receiver of the message perform mutual authentication to ensure the transmission is directed to the appropriate recipient.
  • Patient Rights protected//upheld: These prerequisites enable a patient to be confident that disclosures of personal health information are properly authorized, and that such authorization is verifiable. The identity of the requesting party is specifically known, and is not anonymous from verification. Users of systems that facilitate making a request for release of information are subject to authorization enabled by access control policies to assure proper access to personal health information. Prerequisites in this area include: [1] That user identities are known and authenticated for requestors of releases of information; [2] That user access permissions are established by access control policies enabled within the systems from which document query requests are made; [3] That positive identification is possible and specific to the initiator of the query whether a person, an organization (location) or a trusted identified application recipient representing the user (or proxied to by the user); [4] That the requestor commits to abide by terms of any applicable patient consent/authorization for release of information; [5] That the user/intended recipient is authorized (and validated) to be the recipient in accordance with patient consent or written authorization, a court order, as permitted by law or regulation, as supported by a manually validated request (such as for a release for law enforcement purposes); [6] That evidence of the authorization exists and can be validated programmatically (through evidence of the authorization provided within the context of the request) or through human procedural verification with identification of the method and responsibility for validation
  • These measures help assure that the request for documents is authorized under proper authority, and that the identity and accountability of the requestor is established and verifiable by the recipient of the request for release of information.
  • Audit trails of disclosures to be enabled: Patients have the right to request an accounting of disclosures of to whom their personal health information has been disclosed. Different types of disclosures may be included in that accounting based on the requirements of prevailing law/regulation and policy. All disclosures need to be made auditable on that basis. The audit trail should incorporate, but not necessarily be limited to, information that identifies the party to whom the disclosure was made, who made the disclosure, when the disclosure occurred, what was the subject matter disclosed and why the disclosure occurred.
  • The above prerequisites are seen as elemental to providing the supporting infrastructure for solicited document query processing to occur in a secure manner that upholds patient privacy and the confidentiality of personal health information.
  • Within the document query message structure itself, there are also several prerequisite requirements that should be in place for a normative document query standard to be successful. These must be contained within the query message structure, and must exist prior to the fulfillment of a query. These include: [1] If the request requires patient permission, then the appropriate means of assuring support for non-repudiation (e.g. through electronic signature or through in person identity verification) and unique identification is required for all participants in the release of information for authentication of patients/legal representatives, witnesses and providers as signatories that may be incorporated on consent forms; [2] Standard identifiers must be included for reference to intended recipients (e.g. such as the National Provider Identifier (NPI) in the US or as appropriate for the use of other external references); [3] Inclusion of the automated release of information up to and including the electronically signed (non-repudiated) release of information itself or, if not fully automatable, then the message structure should include the identity of the individual performing the external validation of the appropriateness of the release and the date/time of the external validation.
  • Implementers should be aware of the significance of ensuring satisfaction of these prerequisites prior to attempting to use the document query messages for support of release of information activities for solicited queries.
  • Medical Records Domain Data Consent Topic - Document Statuses and Transitions.

Consent Tracker Breadth of Scope

Consent Tracker scope, as listed below, is constrained during implementation to applicable policies. I.e., in some jurisdictions, there may be no opportunity for a patient to consent or dissent to uses of information or activities performed, either because there is no express consent or consent is implied/assumed.

For example, many jurisdictions collect, access, use, and disclose health care information without consent or implied consent for certain public health, safety, and legal purposes.

Consent Tracker Subjects

Persons who are the subject of information or activity governed by a consent directive.
Consent Tracker Disciplines

- Any type of patient or subject specific health care provision, including physical, preventive, palliative, hospice, community-based, reproductive, maternity, neonatal, pediatric, geriatric, mental, behavioral, substance use, clinical trials, and public health
- Any type of patient or subject specific administrative or financial activities permitted or required for purposes care delivery management, operations, or payment
- Any secondary use of patient or subject specific health and administrative/financial information, including research, public health surveillance, immunization and cancer registries, quality measures, payment incentive programs.
- Any patient or subject specific provision of services, such as health device platforms, or health and fitness APPs.

Care Delivery Environment

Any care delivery environment, including Community, Geriatric, Hospice, Home care, Emergency, Inpatient, Intensive, Neonatal, Pediatric, or Primary Care

Locale

Any jurisdiction in which consent directives are permitted or required by policy.

RIM scope

RIM Classes: ACT, DOC, CACT, OBS

- Act.classCode = ACT, DOC, CACT, CON, POLICY, DOC, TRFR, OBS
- Act.statusCode
- Act.confidentialityCode:
  - Definition: Privacy metadata classifying an Act according to its level of sensitivity, which is typically based on a jurisdictional or organizational analysis of applicable privacy policies and the risk of financial, reputational, or other harm to an individual or entity that could result if made available or disclosed to unauthorized individuals, entities, or processes.
  - UsageNotes: Confidentiality codes may be used in security labels and privacy markings to classify an Act based on its level of sensitivity in order to indicate the obligation to ensure that the information conveyed by the Act is not made available or redisclosed to individuals, entities, or processes (security principals) per applicable policies. Confidentiality codes may also be used in the clearance of initiators requesting access to protected resources.
  - Confidentiality codes may be used by access control systems to match the classification of an initiator's clearance to the classification of the information conveyed by an Act class; e.g., the confidentialityCode is used to convey the classification clearance level required to access information about a sensitive reproductive service.
  - In order for the matching logic to determine dominance of a clearance, which is required to access classified information, the confidentiality codes must cover the breadth and depth needed to support implementation of privacy and access control policies. More specifically, the confidentiality codes must be in a comprehensive set going from least to most confidential, and the set of codes must be "complete", that is, there can be no missing or overlapping levels of confidentiality from a policy perspective. This use should be considered in selecting the value set bound to this attribute, and the binding should be done as Coded No Extensibility (CNE) to allow for such processing.
  - Map: Definition aligns with ISO 7498-2:1989 – "Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes."
- Participation.typeCode = AUTH/RCV; Participation.functionCode = d:AuthorizedParticipationFunction
- Observation.observationValue = SecurityObservationValue

Resource appropriateness

- Consent Tracker represents well understood and mission critical privacy and security concepts in the business of healthcare, as evidenced by mapping to current HL7 standards, ONC projects, and several large state and federal HIEs.


- Consent Tracker has 19 core elements, and works in loosely coupled, wide exchange ecosystems as well as tightly coupled narrow exchange ecosystem, and is intended to support interoperability across, which is why an adequate yet extensible set of FHIR value sets are bound to its CodeableConcepts.

Expected implementations

Content sources

- Intra-Enterprises such as hospitals or integrated provider organization networks such as the VHA
- Inter-Enterprises such as centralized and federated health care organizations utilizing exchange networks such as Health Information Exchanges (eHealth Exchange), DIRECT HISPs, SAMHSA sponsored Consent2Share Behavioral Health Information Exchanges, and electronic Consent Management Systems such as the MIHN eCMS.
- May be piloted as part of the ONC Patient Choice Technical Project
- See FHIR Consent Directive Reference gforge document page for multiple example US and international forms and use cases.

Content sources
Example Scenarios

- Could be used to track and manage BHITS FHIR Consent Directives per the IG and samples below: FHIR Consent artifacts are released on the CBCC GForge project site and HAPI FHIR Java source code is checked into SVN: DSTU2 FHIR Implementation Guide for BHITS (includes profiles for Contract, List, and Basic resources)

BHITSConsentImplementationGuide.implemenationguide.xml BHITSConsent.structuredefinition.xml

- Basic, Research and Granular Consent Directives
  - PrivacyConsent_basic_opt_in.xml
  - PrivacyConsentTest_granular.xml
  - PrivacyConsent_research.xml
- Sample HAPI FHIR client code (DSTU2) available in SVN (as integration and unit tests):
  - iExHub/iexhub/src/main/java/org/iexhub/services
  - iExHub/iexhub/src/test/java/org/iexhub/services

Resource Relationships

- Consent Tracker Resource is not a Consent Directive. As has been the case with other Consent metadata management/tracking capabilities in the standards listed above, it separates the management from the actual contract to minimize unauthorized disclosure, while conveying sufficient metadata to locate/retrieve, and enforce access control policies based on confidentiality and security control security labels per the HL7 Data Segmentation for Privacy Exchange/Direct Implementation Guides.


- Consent Tracker supports, but does not duplicate the Consent Resource any more than any standard for consent directive management duplicates the referenced consent directive. It conveys the consent directive metadata. For example, Consent Tracker does not specify the authority, domain, granor, grantee, signature, restriction or extension provisions that constrain the Consent Directive class, or the activity or activityReason permitted or denied a named agent. If an end user needs more specific information than is included in the Tracker metadata, then the user will need to access the consent directive or surmise from the Consent Directive Type the policies included in the Consent Directive instance.
- Unlike Consent Resource, Consent Tracker uses Codeable Concepts from extensible value sets based on recognized standard vocabulary, and in the case of Consent Directive Type value set, both standardized codes and recognized Consent Directive forms.
- Consent Tracker and Security Labels:
  - Consent Tracker Resource instance has its own optional security label metadata, in keeping with guidance in V2 ARV - "System implementers should carefully control access to the restriction codes and values, as they themselves hold sensitive information."
  - Unlike Consent Resource, Consent Tracker optionally conveys the Consent Directive Confidentiality label, which an authorized recipient will be provisioned as a clearance attribute
  - Unlike Consent Resource, Consent Tracker optionally conveys the Consent Directive Security Control labels to which an authorized recipient must comply.
  - Unlike DocumentReference, Consent Tracker does not include sensitivity Security Labels as these may be privacy leaking to end users who are authorized to access or retrieve some Contract Tracker Resources, but who may not possess the security clearance attributes permitting them to access the Tracker of an additionally protected Consent Directive. E.g., a dietician who is a member of a patient's primary care team may not be provisioned to access the patient's mental health information.
  - Could be included in or leveraged by the FHIR Privacy Consent Directive Implementation Guide [PCD], which is intended as a framework of FHIR Privacy Consent related Resources and Profiles. The PDC roadmap includes development of a FHIR Consent Directive Questionnaire /Questionnaire response profile, which may be linked to a FHIR ConsentDirective profile in order to populate the relevant FHIR ConsentDirective elements for a computable ConsentDirective that remains linked to the Patient Friendly Consent Directive form in which the patient/subject selects asserted or disclaimed to provisions. This enables a data subject, collector, and processor to maintain links to the patient's informed consent for purposes of updating, renewing, or rescinding that agreement.
  - Could reference the location of a paper consent form, a v.2 CON Segment, a v3. Data Consent Message, a CDA Consent Directive, a FHIR privacy, medical, research, advanced directive etc ConsentDirective profile or the proposed Consent Resource for purposes of retrieval or audit.
  - Could be leveraged for conveying consent directive privacy protective metadata in a federated, wide ecosystem by the pending [1] FHIR Profile Proposal, which is described as:

It is defining an IG for an ecosystem that is following the IHE White Paper on “Document Sharing”, which is the abstract model for what XDS started but has gone well beyond XDS. • A document Sharing environment equally handles all kinds of documents, it is not constrained to CDA or FHIR documents. • This is a working ecosystem, including patient management, patient cross referencing, User management, access controls, audit controls, provenance requirements, and eventually consent. • This ecosystem will be constrained following the IHE White Paper, and should be able to be standalone as well. That is that it is envisioned to be equally an API to an XDS ecosystem, or deployed as a standalone Document Sharing system purely FHIR based. • This IG will leverage existing IHE profile of the current profiles that use FHIR (MHD, PIXm, PDQm, ATNAm, and MHD-I), use of IUA, and likely future Consent profile.

DRAFT Consent Tracker Resource Spreadsheet and Value Sets

- Draft Consent Tracker Resource Spreadsheet
- Consent Directive Recipient value set
- Consent Directive Class value set
- Consent Directive Type value set
- Consent Directive status value set

Timelines
Complete Resource and have approved for submission prior to July 17, 2016 Ballot Freeze date.

**gForge Users**
Paul Knapp, John Moehrke, and Mohammad Jafari