*Regional EHR  
design issues - Consent*

**openEHR**



**Date** Mar, 2016  
**Prepared By** Thomas Beale  
 Ars Semantica

**Copyright 2018 Ars Semantica**

This document may be shared and reused, as long as attribution and integrity are maintained, according to the CC-BY 3.0 unported licence.

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Description** | **Author** | **Date** | **Version** |
| Initial Writing | Thomas Beale | 01 Apr 2017 | 0.9 |

**Disclaimer**

Ars Semantica makes the information and other material (“Information”) in this document available in good faith. Ars Semantica cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

**Trademarks**

Company, product, and service names mentioned herein may be trademarks or service marks; such marks are the property of their respective owners.

# Consent Concepts

## Conceptual Definition

The notion of ‘consent’ while commonly used in health IT is often not well defined. There are various definitions of the term ‘consent’:

* **Medical consent**: consent by the patient, guardian or other legal person for a (typically major) medical procedure or other intervention, e.g. involuntary psychiatric admission, end of life support, organ donation etc;
  + Patient preferences such as refusal to accept blood transfusion, organ transplantation may be considered as similar to medical consents;
* **Point of care information sharing / use consent**: consent by the patient or legal representative, or in emergencies, health care personnel, for access to the patient heath record or related data (lab test results etc) – linked to the patient, aka ‘identified’ data;
* **Secondary use information sharing**: consent for use of pseudonymised or otherwise de-identified health data, normally for public health, statistical or research uses.

Medical consent and information consent are two different concepts, and for the purposes of the shared EHR, we are interested in the latter.

In terms of a shared EHR, we assume that:

* The primary information is identified or linkable to the patient, for purposes of care delivery;
* That pseudonymised and/or completely de-identified forms of the information are or would be derivable from the primary information for secondary use.

Therefore, consent for access and/or sharing of both identified and de-identified forms of the information are relevant to the shared EHR.

It is assumed that the two kinds of consent are sufficiently different that different models and technical means or at least distinct rules, documents or procedures may be required to implement them.

## General Paradigm

The underlying need being served by a patient consent function in an EHR is to maintain patient privacy outside of use of data by health professionals in a care delivery situation. Consent is thus an information access and sharing control concept, i.e. it is to do with authorised access and uses of patient data. For the concept to have any meaning, there must be means of:

* Determining whether a particular request to access is legitimate;
* Allowing legitimate access;
* Blocking unauthorised access.

In general it must be assumed that any system of controlled access can be broken, therefore it must be further assumed that unauthorised access should be detectable.

# Requirements

## Who can access the data?

The general notion of consent for access to health data for care provision can be understood via a term used in the UK, ‘legitimate relationship’. This concept recognises that only HCPs having an established care relationship with the patient can access the information. These HCPs include:

* HCPs in long-term relationships, e.g. general practitioners, outpatient services;
* HCPs in acute care setting including named consultants, specialists, and changing ward staff;
* Specialists;
* HCPs in the emergency services, i.e. ambulance, other rescue services.

In the case of emergency services, the relationship may be established by the relevant personnel obtaining access under a ‘break glass’ condition in which their access is logged in detail, and justified by immediate need.

There is usually a need for other persons who are not HCPs to have access to the patient data, such as administrative staff, legal representatives etc, but it can usually be assumed that access to data in a shared EHR is related to a patient encounter at which a physician will be present.

Another useful term, equivalent to the ‘legitimate relationship’ concept is ‘attending physician’, which means any physician (including midwife) who is providing care, no matter what their particular employment role is.

For secondary use, the users of the data are typically defined in terms of organisations, e.g. a university, a hospital, a government or a company.

## What are the data used for?

For healthcare delivery the data use is clear – it is for enabling clinical professionals to perform their normal functions.

In the case of secondary use, consent is normally for the use of the data for specific purposes, and it is normally assumed that the patient can assign rights on the basis of the intended recipient and use. Uses include:

* public health (e.g. for diagnoses of major conditions to be counted),
* medical research (use of cancer treatment data for a university hospital study);
* use of health data by pharmaceutical companies for development of drugs.

Clearly the beneficiaries, both in terms of health and financial, may differ widely, and so consumers may expect to allow selective access.

## Which data can be accessed?

In some models of consent, there is a concept of ‘sensitive’ and ‘non-sensitive’ data. Sensitive data typically include those data that may be socially stigmatising (e.g. HIV diagnosis, mental health involuntary admission) or thought to be compromising e.g. for health insurance purposes (e.g. pre-existing or genetic conditions), but might in theory include any data the patient nominates.

Clinically speaking, it is difficult to separate out sensitive and insensitive parts of the patient record, since most of the managed lists and other longitudinal data – problem list, current medications, allergies etc – are likely to contain items that relate to supposedly sensitive conditions, e.g. HIV, psychiatric prescriptions etc.

IT professionals often fantasise that the contents of the EHR can be sliced up and assigned differential access rights, but in reality, any such scheme risks a) being incomprehensible to its human users; b) technically complex and c) non-interoperable.

## Access logging and sanctions

Access can be controlled by technical and social means. The technical approaches include various typical access control systems which are based on implementing rules based on some or all of the above-described aspects of data access. These are noted below. However, social control can also be exerted by use of global EHR access logging and advertising this fact. This provides a means of determining after the fact whether particular accesses were in fact legitimate.

## Differential access to EHR Data

Differential access to EHR data is a common concept in e-health. A basic division between administrative content, e.g. content captured at admission, for bookings etc, and clinical content. Within clinical content, a typical intention is to enable principle HCPs, i.e. consultants, primary GP etc, to see the whole EHR but to limit the visibility of data to e.g. ward nurses. Various schemes to effect such access have been described.

### Content based access

In the shared EHR, it is proposed in one analysis that the following categories of data exist:

* Administrative – not considered a separate data set in the original analysis (REF) but necessary if administrative staff are to be able to work with patient record without seeing clinical information;
* Emergency – core data set sufficient for emergency care;
* Shared – a wider subset of EMR data sufficient for more routine care;
* Complete – an EHR that is clinically speaking the same level of detail as a typical institutional EMR.

It is assumed that shared EHR systems will initially accumulate ‘emergency’ data, then ‘shared’ data and over time grow to the ‘complete’ level. Practically speaking however, things are not so simple: different source institutions will be able to provide different types of data at different times, and for different types of patient, which data belong in each category is not likely to be identical.

Thus, while it has been proposed to mark data in the EHR as belonging to each category, in order to enable differential consent. However, this is likely to prove problematic, and is not recommended. It would thus not be useful as a basis for consent.

Therefore, we are likely to be left with just the division of administrative and clinical data as a basis for content-consent. Within an openEHR EHR, this is relatively easy to implement, since administrative information is normally recorded only in ADMIN\_ENTRY data items.

### Access based on sensitivity

Alternatively the ‘sensitive/other’ notion of the EHR could potentially be implemented to enable differential access control. However, as for the emergency/shared/complete division, a detailed model is difficult to devise. Such a model would require a special part of the EHR to which certain data could be added. There are certainly some types of data that health consumers might reasonably want to hide, such as previous admissions to psychiatric institutions, encounters in prison health services etc. The danger is that the clinical integrity of the health record may be compromised by inappropriate use of such a mechanism, for example, if certain diagnoses or medications were to be moved to the sensitive part of the record.

Assuming such a facility could be made to function properly in the sense of clinical semantics, a technical design would be required. This might be based on a ‘locked vault’ concept, where an extra key was required to access the contents of the vault, or some other scheme.

As previously noted, any scheme must be implementable and understandable by users.

### Manually controlled access of committed items

Another way to control access to EHR data is to enable marking of individual committed data items as being accessible to certain parties. This is likely only to work for an EHR that consists of well-defined commit items, such as openEHR, or document-based EHR systems. In an openEHR system, that unit of visibility would be the Composition version.

One scheme for doing this was developed by the Estonian e-Health program (see ref below), as follows:

* Items visible with no access restrictions;
* Items closed by a clinician
  + Includes items that may only be made visible to the patient after review with doctor, and items that may never become visible to the patient;
* Items closed by the patient
  + Documents hidden from clinicians
  + Documents hidden from legal representatives (e.g. parents, guardians) but visible to clinicians.

This scheme would be implementable within an openEHR health record, although whether it is useful to do so remains a question, since there is always the question of: what data, if hidden, will compromise healthcare delivery?

Again, although not described specifically as part of the scheme, it is most likely that administrative data should be accessible differently from clinical data.

### Roles

Differential access to content relies on a system of roles, i.e. kinds of employees and/or their function in a consultation or in-patient care episode. Even the simplest system of content control requires some roles to be identified, as follows:

* Patient
* Patient’s legal representative, if applicable (e.g. family member with power of attorney)
* Patient’s health representative / guardian, if applicable (e.g. parent)
* Physician in care delivery relationship (i.e. with ‘legitimate relationship’)
* Administrative staff member.

Defining the ‘physician’ category as any registered physician in a care relationship with the patient (i.e. for which the physician’s HCF has a mandate for care from the patient) is a useful simplifying principle compared to trying to use ‘hard’ roles such as ‘GP’, ‘consultant’, ‘on-call physician’ etc.

Note that physicians in any setting, including schools, prisons, military, and also midwives working solo would all be considered as physicians in a care delivery relationship with the patient.

Other roles that may need to be considered separately from those of the attending physician:

* Pathologist, e.g. after patient death, for autopsy etc;
* Forensic medical specialist, in specific cases, e.g. major adverse events and death, criminal investigations;
* Pharmacists: it is unlikely that a pharmacist not working directly with an attending physician should be able to see the record, but there may be a need to implement a capability to check medication interactions which might be available to the pharmacy, without the underlying data being made directly visible;
* School healthcare employee: some restricted rights, e.g. to emergency data, vaccination list might make sense, depending on what situations can occur in the school setting.

## Access to in-situ data versus serialised data (messages etc)

The discussion so far pertains to live access of data by users or other systems, and assumes that as soon as the user or other system logs out or drops contact, no persistent form of the accessed data remain in uncontrolled location.

This leaves two problems to be resolved:

* Local (device-side) capture or caching of data – this might be both legitimate, e.g. to allow offline health workers to work, and malicious;
* How consent for messages between systems should work.

In the first case, legitimate caching would require encryption based on an authorised user and authentication method, ideally with a time-limiting mechanism as well.

### Consent for B2B communication (messages)

In an environment where messages are sent between systems, some form of consent is likely to be required. Messages that occur in routine care, such as sending of lab results, radiology etc, would normally be encrypted within a PKI or similar kind of system, in which private / public key pairs are used by sending and receiving systems.

The easiest way to represent consent for patient data to be transferred in messages is probably as follows:

* For in-patient care episodes, include extra conditions on the main consent document created at admission that state:
  + that the admitting institution may send and receive messages containing identified patient data to specific data partners for clinical care purposes;
  + that all transmissions to such data partners are encrypted, and that the admitting institution guarantees the same privacy conditions as for internal (EMR) data;
* For general practice / family clinics, a time-unlimited condition to enable messaging for clinical care purposes can be included, with the same specifics as above.

This approach makes the primary institution or clinic in each case responsible for privacy of patient data in messages, and holds them legally responsible in the same way. It also gives them the freedom to change data partners without informing the patient, as would been needed if a new pathology lab is connected to a hospital.

# Practical Considerations

## Point of care

A system of consent for a shared EHR needs above all to be understandable by users and implementable in software and data.

Underlying principles that may be used for primary (healthcare delivery) uses are:

* most citizens prefer to provide open access to HCPs in a legitimate relationship during a period of care, and for the health record to be otherwise maintained private;
* most citizens accept the need for emergency HCPs to obtain access to the patient record without the usual consent negotiation, if this is not possible, i.e. emergency access;
* it is assumed that global EHR access logging is in place, and that any access (read or write) is logged in a permanent way, with the HCP user id, name, date and time, location and technical address (typically device type, name and IP).

### Simple ‘claimed consent’ model

On this basis, consent for a shared EHR could be managed by providing the means of:

* consent to be recorded for use of the health record at the commencement of any *encounter* (primary care, specialist, laboratory etc) by the senior HCP and is assumed to stand for other participating HCPs from the same HCF (e.g. family clinic) for the period of the encounter;
  + an ‘encounter’ is assumed to be completed when the patient leaves the HCF;
  + the consent is enabled by the patient or legal representative signing in some way;
* consent to be recorded for use of the health record at the commencement of an *episode of care* (hospital, other long stay institution) by a responsible clinician, and is assumed to stand for all other users in the same institution (HCF) for the period of the episode;
  + an ‘episode of care’ is assumed to be delimited by admission and discharge events;
  + the consent is enabled by the patient or legal representative signing in some way;
* consent for emergency access to be unilaterally obtained by HCPs for emergency use; in this case, the relevant HCPs need to provide reason for use, and identifying information;
* marking a recorded consent as being ‘closed’ due to the end of the encounter or episode – any consent not ‘closed’ is considered ‘current’;
* the HCF of any accessing user (i.e. HCP) to be determined, and to be used to block users not from a the HCF authorised for the current episode;
* using a previously recorded current consent to determine whether a new access request by a user X from HCF Y during time period T1 – T2 should be allowed.

This approach can be understood as a ‘claimed consent’ approach i.e. consent is claimed each time care is provided. In the simplest form, it is assumed that data access is ‘all or nothing’.

More complex schemes would try to introduce computable rules representing long-running relationships, as well as differential access to different parts of the EHR.

### Care team consent model

For some (e.g. chronic) patients it may make sense to implement a ‘care team’ model of consent, where the consent to access covers a list of named HCPs, potentially from different institutions. This kind of consent would be used to enable long-term (possibly indefinite) access by trusted long term carers to all EHR data for the patient. It would require a way of modifying the care team list (i.e. adding and deleting members).

In this scheme, if a care team consent was present, it would be checked first by the access control system for allowing access, otherwise consent would revert to the ‘claimed consent’ model above.

## Secondary use

For secondary uses, the following principles can be assumed:

* most citizens prefer to *enable* routine public health and public research use of their de-identified data – in some countries, this may be legally required in order to use public healthcare;
* most citizens prefer to *control* the use of their data for commercial secondary use, e.g. by pharmaceutical companies.

These considerations imply different consent approaches for public versus non-public use.

### Public health system

On this basis, it would seem reasonable to implement the following within the public healthcare system context:

* a consent for global unlimited use of de-identified data, strictly within the public health system, possibly with consent automatically created on an opt-out basis;
* de-identified / summarised data for public health use is computed and potentially cached in a location only accessible to authenticating public health systems.

### Research and commercial

For most other secondary uses it is assumed that a particular organisation (i.e. institution, company etc), and usually a ‘study’ (e.g. clinical trial) is implicated in which de-identified or pseudonymised data are requested. Accordingly such requests for use should be represented by a separate kind of consent designed for ‘non-public health use’. In this case, the consent should describe the specifics, i.e.

* Which institution;
* What data are requested;
* For what purpose – study etc;
* Time period;
* Commercial gain;
* Ultimate beneficiaries.

A legal document should potentially also be included which obliges the requesting institution to remove all data once the use has expired.

# Consent service design

Possible service functions:

* View consents (with various filters)
* Create a consent (type, HCF, HCP(s), patient, time, content types, …)
* Revoke a consent (id)
* Add an HCP to a consent

## Consent Update Model

Consent settings will in general change over time, and it is crucial to have model of consent that accommodates the idea of updates to current consents, including various kinds of changes, additions and deletions. The information model of consents must therefore be based on enabling updates to be integrated in order to form each new ‘state’ of the consent data, that remains coherent.

TBD: more

## Consent Consistency

Related to the above, it is essential that the full set of consent information for a subject be internally coherent and consistent. That means that each change that is applied must result in a new consistent state. Some formal rules are required to ensure this.

TBD: more

# Consent Information Model

An information model of consent includes various parts. The general concept is that a ‘consent’ is a structured document containing human-readable text, signatures and potentially various computable elements, such as identifiers of HCPs, time-limits etc.

According to the discussion so far, the following separate consent document types might be defined. The following sections provide only suggestions and do not constitute a considered design.

## Consent for Access and sharing of health data for Care provision

The core information structure might be designed as follows:

* Identifier
* Title:
  + Consent for health data use by <HCF>
* Subject:
  + Name
  + Identifying information
  + etc
* Assigned to Healthcare Facility (HCF)
  + Facility name
  + National health provide identifier
* Description:
  + E.g. this consent covers use of health data for care provision purposes.
* Rights granted
  + Access to identified health data held by HCF during care provision period by HCF clinical personnel
  + Right to transmit and receive health data to and from identified data partners for clinical purposes
  + Issuing recalls / reminders
  + Outpatient use …
  + etc
* Consents (list)
  + HCF Consent
    - {id = patient id + HCF id + ??? // needed to match revocations}
    - Content specification
      * Confidentiality level
      * Clinical time range of data
      * Etc.. e.g. particular queries etc..
    - Period [1]
      * Start date / end date | until date | from date | open
    - Expiry [0..1]
      * Date time representing maximum period of this consent, even if open.
    - Assigned HCF [0..1]
      * CNES id
    - Assignees of consent – one of:
      * Responsible HCP(s)
        + Name
        + CNS id
      * Department [0..1]
        + Role(s)
        + Id (CNES)?
    - Assigner of consent
      * Patient | legal guardian | relative | power of attorney
      * Details
    - Signatures
      * Xxx
  + Named individual consent
    - {id = patient id + ??? // needed to match revocations}
    - Content specification
      * xxx
    - Period
      * Start date / end date | until date | from date | open
    - Expiry
      * Date time representing maximum period of this consent, even if open.
    - Assigned HCF [1]
      * CNES id
    - Assignees of consent – one of:
      * Guardian [1]
        + Identifying info
        + Legal basis for claim to guardian rights
      * Legal representative
        + Identifying info
        + Legal basis for claim to be legal representative
    - Assigner of consent
      * Patient | legal guardian | relative | power of attorney
      * Details
    - Signatures
      * Xxx
  + Consent
    - …
  + Consent revocation
    - …
  + etc

Using this model, the ‘consents’ list at the end would be added to with a specific consent each time a health system contact occurs. This would reduce the amount of consent documentation added to the EHR.

TODO: deal with care team concept

TODO: deal with revocation

## Consent for Sharing of de-identified data for public healthcare

TBC

## Consent for Research use of health data

TBC

## Consent for Commercial use of health data

TBC

# References

<https://www.ttu.ee/public/k/Kliinilise_meditsiini_instituut/AccessRightsandOrganizationalManagementinImplementationofEstonianElectronicHealthRecordSystem.pdf>

References: <http://www.digitalhealth.gov.au/using-the-my-health-record-system/maintaining-digital-health-in-your-practice/patient-consent>