OpenHIE Discussion Document

Consent Management

Doc-To-Help Standard Manual

Derek Ritz
ecGroup Inc.
Draft 0.1: 2015-04-13



<http://www.ecgroupinc.com>

+1 (905) 515-0045

Contents

Overview 1

The problem… 1

Key challenges associated with this problem 2

Opt-out vs. opt-in 2

PHI collection vs. disclosure 3

Authentication vs. authorization 3

Public vs. personal interests 3

Clinical risk vs. privacy risk 4

All ya gotta do is… 5

1. Implied consent; all-in or all-out; no BTG 5

2. Implied consent; all-in or all-out; support BTG 6

3. Explicit consent; all-in or all-out; no BTG 7

4. Explicit consent; all-in or all-out; support BTG 7

5. Implied consent; segmented disclosure; support BTG 8

Technical Designs 10

Design overview 10

Related IHE profiles 10

OpenHIE architectural elements 10

# Overview

## The problem…

The distinct concepts of privacy, consent, confidentiality and security are related to each other. **Privacy** is a human right of self-determination; “…[i]n relation to information, privacy involves the right of individuals to determine when, how and to what extent they share information about themselves with others.”[[1]](#footnote-1) **Consent** is an individual’s voluntary agreement to share his or her PHI. **Confidentiality** is “[the] property that information is not made available or disclosed to unauthorized individuals, entities or processes.”[[2]](#footnote-2) **Security** is the “preservation of the confidentiality, integrity and availability of personal health information.”[[3]](#footnote-3)

At present (OpenHIE v1) there is no support for *consent management* in OpenHIE. There is basic security and support for confidentiality. Through OpenHIE’s adoption of ATNA (IHE’s Audit Trail and Node Authentication profile) it can be assured that the Interoperability Layer (OpenHIM) “never talks to strangers”. For any authenticated node, however, OpenHIE supports 100% access to 100% of the content in the HIE.

In this situation, the “policy posture” of OpenHIE is that it supports *implied consent[[4]](#footnote-4)* on the part of subjects of care that all of their personal health information (PHI) may be collected and stored in the HIE and that it may be made available to any *authenticated* health worker to support care delivery (OpenHIE’s primary purpose of use). Importantly, the authentication of health workers is not enforced by OpenHIE. OpenHIE relies on the capabilities of point of service (POS) applications to enforce the authentication of health workers. It may reasonably be assumed to be an aspect of “on-boarding” a new POS that it is demonstrably able to do this end-user authentication *before it is accepted as a known and trusted node on the HIE*.

The gist of the present issue is that the very concept of privacy relies on there being a supported capability for a subject of care to withdraw their consent. Defined this way, today, OpenHIE lacks any support for privacy.

## Key challenges associated with this problem

There are a number of challenging dimensions surrounding issues of consent:

* Opt-out vs. opt-in
* PHI collection vs. PHI disclosure
* Authentication vs. authorization
* Tensions between public vs. personal interests
* Clinical risk vs. privacy risk.

### Opt-out vs. opt-in

It is a basic question of policy whether there is an implied/deemed consent[[5]](#footnote-5) to share PHI based on the very act of care-seeking behaviour. Such a consent model operates on the premise that patient-safe, high-quality care delivery relies on the maintenance and sharing of PHI and so it stands to reason that anyone who presents for care would have an expectation of such data sharing and need not explicitly consent to it. Furthermore, since continuity of care relies on the sharing of PHI over time and across different sites of care, such implied consent may reasonably be taken to extend to an HIE.

Implicit consent is also known as “opt-out”. This is because you don’t need, under an implicit consent policy, to opt “in” before your PHI can be collected and shared for care purposes (and certain related purposes). Under implicit consent, you invoke your rights of privacy by opting *out*.

Implicit consent is in natural tension with its counterpart: explicit consent. An opt-in policy requires that each patient explicitly provide informed consent prior to the collection and sharing of PHI. Such a policy gives operational effect to the person-centric healthcare tenet: “nothing about me, without me”. Explicit consent gives primacy to the “personal rights” aspects of privacy.

One of the key challenges regarding opt-out vs. opt-in is the relative effort (and associated cost) of operationalizing each option. Capturing informed, explicit consent is difficult, time-consuming, and expensive. There are also studies which have shown that the “enrollment” rates of opt-in schemes are significantly lower than for opt-out schemes.

A key challenge for opt-in schemes is to be very clear about exactly **what** is being opted into. Because the consent is implicit, there is a *reasonableness* test that must be passed in order for there to be public acceptance of the policy. Most citizens, for example, will be fine with their PHI being used to directly provide high-quality care to them and to support the financial and health system management processes needed to effectively and efficiently deliver these services. Many, however, would expect to have to explicitly consent to their data being used (for example) by commercial entities for marketing purposes.

### PHI collection vs. disclosure

There are some who believe that there should be consent required to *collect* PHI as well as to disclose or share it. Others contend that the collection of PHI is not something one can choose to opt out of as it is necessary to support payment processes and health system management processes which accrue to the benefit of the subject of care and which, themselves, are non-optional. There are also public health and surveillance workflows that cannot be opted out of, such as the tracking of certain reportable diseases.

The common notion of “consent” is more precisely defined as a “consent to disclose”. A key challenge regarding the very idea of “consent to collect” is that the withdrawal of such consent undermines the many companion workflows that go with care delivery. On the flip side, requiring a consent that cannot be withheld is an ethical quandary. Under such circumstances, the withdrawal of consent to collect becomes tantamount to a withdrawal of consent to treat. Notwithstanding these very real issues, the concept of “consent to collect” is held dear by some libertarians.

### Authentication vs. authorization

Authentication is proving that a party is who they purport to be. OpenHIE’s use of ATNA, for example, allows the Interoperability Layer to authenticate that the communicating node “is who it claims to be”. Extending OpenHIE’s authentication to the subject of care or to the health worker requires a degree of engagement with this party that, today, is foregone in favour of trusting the POS’s ability to establish and enforce end-user authentication. Leveraging this trust network – the POS purports the authenticated end-user and OpenHIE accepts it as true.

Authorization is a natural follow-on to authentication. Authorization is establishing, for a known party, what it is that they are allowed to do or are allowed to see. A consent directive that is more finely grained than all-access / no-access will rely on the authenticated identity of subjects of care, providers of care, or both – so that authority to access PHI can be established. Even role-based access control (RBAC) relies on establishing identity since the role is an attribute of the identity.

Authority can reside within a context as well as with a person. In many jurisdictions, a clinician (role) in an emergency room (context) may be able to circumvent consent directives by metaphorically “breaking the glass” (BTG). A BTG, when it is invoked, often is supported by an explicit audit record which logs the clinician’s BTG decision and the reason for invoking the override.

In some jurisdictions, a clinician’s right to BTG is supported by the medicolegal risks such professionals assume and their overarching duty of care which, as a matter of policy, may “trump” personal privacy concerns. Under such circumstances, a subject of care’s right to privacy is subjugated to a care provider’s right to access full information in support of safe, quality care delivery.

### Public vs. personal interests

At the outset, it must be said that one of the expected benefits of investments in pervasive eHealth infrastructure is that it supports patient-safe, high-quality care delivery at scale. Such care is, for each individual, very much in their personal interest. In aggregate, the sum of these personal interests represents a public interest. In jurisdictions where some of all of care delivery is publicly funded, an eHealth investment can therefore be seen as contributing to a common good.

An individual’s interests as regards to personal privacy may be in tension with the public good. A case in point is HIV (or Ebola), which is a reportable disease diagnosis in many jurisdictions. Where an individual’s diagnosis is deemed to have a public health impact, the public’s rights to health protection are given precedence over the individual’s personal rights of privacy.

One can also make a case that expenditures on eHealth infrastructure are made out of a “common pool” (a single healthcare budget) and so costs for eHealth infrastructure or eHealth operations have an opportunity cost as well as a financial cost. This can be important when considering a complex/expensive privacy solution versus a simpler/cheaper one. The added complexity (and its incremental value, if it extends system functionality) will accrue to the benefit of individual interests, but possibly at the expense of public interests. Such considerations are especially germane in situations where the number of persons availing themselves of consent management solutions is very low compared to the overall population of system subjects.[[6]](#footnote-6)

### Clinical risk vs. privacy risk

*Level of risk* is defined as the product of the likelihood of an event times the impact or consequences of the event (where both may be expressed quantitatively).[[7]](#footnote-7) One of the key challenges when evaluating privacy risk is to develop a metric indicative of the potential impact or consequences (the level of harm) that may be associated with a breach in the privacy of PHI. Where there is a tension between privacy risk and clinical risk, the situation is made difficult by the fact that it is very much an apples-to-oranges comparison. Clinical risk can be truly life-threatening and this is a fundamentally different order of harm than what is generally considered to be associated with privacy risk.

Such comparisons of risk become important when designing and implementing an eHealth system’s “default” behaviours. By way of example, there is a concept in process engineering called “fail-open” vs. “fail-closed”. The terminology arose from the days of process engineering when designers had to mitigate risks due to lost signal (due to an electrical power failure, for example). The distinction used to refer to which side of a butterfly valve the spring was on; when the power went out, did the butterfly valve spring open or spring closed?

Such an analogy can be applied to the design of eHealth infrastructure. In the absence of a signal – when there is doubt or ambiguity about a subject of care’s consent directive – does the PHI get disclosed (fail-open) or is it kept private (fail-closed)? In answering such a question, one must weigh the clinical risks (which are mitigated by failing open) vs. the privacy risks (which are mitigated by failing closed).

This issue is related to the earlier break-the-glass (BTG) discussion. A subject of care’s desire to withhold PHI from a care provider is completely unrelated to whether or not that PHI is germane to safe, high-quality care delivery. Stigma and embarrassment are the key motivators regarding decisions to withhold PHI and these can be, paradoxically, the most clinically relevant pieces of information. HIV is a classic example of such a stigmatized condition. There are almost no clinical situations where knowing a person’s HIV status is irrelevant and yet a stigmatized patient may not want to share that diagnosis with anyone.

## All ya gotta do is…

This section is intended to connect consent management challenges, and the options that may be favoured to address those challenges, to technical and sociotechnical designs that give these options operational effect. The title of the section is reflective of the author’s decades of experience working to map technical solutions to sociotechnical problems. Often, these technology-centric solutions were introduced by engineers with the phrase: “all ya gotta do is…”.

Unlike the previous sections in this document, in this section there is a course of action which is strongly favoured by the author. This makes this section read somewhat like a persuasive essay and so it should likely be taken with a “grain of salt”. The favoured option is listed first. Other options are also explored, but it will be sometimes evident from their description that these options are not preferred for various reasons usually related to the increase in solution complexity/cost as compared to the relative increase in value.

### 1. Implied consent; all-in or all-out; no BTG

No POS software changes required. Can leverage population-level education regarding privacy. Opportunity for paper-based workflows to support sparse “opt-out” population. Immediate population benefits and network effect at “go-live”; no waiting on the ramp-up of consenting subjects.

The recommended consent management option for OpenHIE is disclosure opt-out (there is implied consent to collect and to disclose). PHI is always collected. In the absence of a disclosure consent directive, 100% of the PHI in the HIE would be returned to the requestor. The point of service (POS) system would be relied upon to authenticate users and to enforce role-based access control (RBAC), if appropriate. Such authentication and authorization would be out of scope for OpenHIE (although may be required as part of the on-boarding process to become a trusted node on the HIE).

A subject of care who opts out would be entirely opting out of sharing any PHI; there will be no support for BTG. A subject of care who opts out “falls back” to care processes unsupported by the HIE (even though episodic PHI is collected about them and saved to the SHR).

All ya gotta do is:

* At the CR, associate a Boolean attribute (a flag) with the enterprise client ID (ECID), which indicates if the client has opted out.[[8]](#footnote-8)
* At the CR, provide a way to set and clear this flag. This could be an administrative maintenance application (it does not need to be exposed to POS applications).
* At the IL, for each query for PHI, check the ECID’s flag; if opted out, return exception; if not opted out, return requested content.
* At the POS, support:
	+ education of subjects regarding their privacy rights and the implications of withdrawing consent to disclose
	+ capture (paper-based or electronic), filing and maintenance of subject’s disclosure consent directive
	+ communication of subject’s consent directive to the CR (electronically, or via a paper-based workflow to a central CR administration).

### 2. Implied consent; all-in or all-out; support BTG

POS software modification is needed to support BTG. Education burden regarding clinician use of BTG. Oversight needed of BTG events. Supports clinician “rights”. Immediate population impact.

This option is the same as option 1 except that break-the-glass (BTG) is supported. If a subject of care opts out, their PHI is not returned as part of a normal query. A POS may, however, resubmit the query as a BTG query and this will override the subject’s consent directive and return all content. Such functionality support clinician “rights” regarding professional and medicolegal aspects, but at the expense of subjects rights to exercise privacy.

All ya gotta do is:

* At the CR, associate a Boolean attribute (a flag) with the enterprise client ID (ECID), which indicates if the client has opted out.
* At the CR, provide a way to set and clear this flag. This could be an administrative maintenance application (it does not need to be exposed to POS applications).
* At the IL, support inbound queries with a BTG flag and BTG reason; save the BTG flag and BTG reason to the ATNA log.
* At the IL, for each query for PHI, check the ECID’s flag and the inbound query’s BTG flag; if opted out and BTG != TRUE, return exception; if not opted out or BTG = TRUE, return requested content.
* At the POS, support:
	+ electronic capture of BTG reason and (re)execution of HIE queries as BTG queries with local electronic audit logging regarding the BTG event.
	+ education of clinician users regarding BTG and its implications
	+ education of subjects regarding their privacy rights and the implications of withdrawing consent to disclose
	+ capture (paper-based or electronic), filing and maintenance of subject’s disclosure consent directive
	+ communication of subject’s consent directive to the CR (electronically, or via a paper-based workflow to a central CR administration).

### 3. Explicit consent; all-in or all-out; no BTG

Administrative burden of educating subjects and capturing and maintaining consent directives. Ramp-up to population benefits.

This option is the same as option 1 except that explicit informed consent (opt-in) is required before a subject’s PHI can be shared. Until a subject opts in, their PHI is not returned as part of a normal query. There is no support for break-the-glass (BTG) functionality.

A subject of care who does not opt in “falls back” to care processes unsupported by the HIE (even though PHI is collected about them and saved to the SHR).

All ya gotta do is:

* At the CR, associate a Boolean attribute (a flag) with the enterprise client ID (ECID), which indicates if the client has opted in.
* At the CR, provide a way to set and clear this flag. This could be an administrative maintenance application (it does not need to be exposed to POS applications).
* At the IL, for each query for PHI, check the ECID’s flag; if not opted in, return exception; if opted in, return requested content.
* At the POS, support:
	+ education of subjects regarding their privacy rights and the implications of providing consent to disclose
	+ capture (paper-based or electronic), filing and maintenance of subject’s disclosure consent directive
	+ communication of subject’s consent directive to the CR (electronically, or via a paper-based workflow to a central CR administration).

### 4. Explicit consent; all-in or all-out; support BTG

Complexity, cost and burden of both patient and clinician education. POS software mods needed. Undermined support for privacy rights. Ramp-up to population benefits.

This option is the same as option 1 except that explicit informed consent (opt-in) is required before a subject’s PHI can be shared. Until a subject opts in, their PHI is not returned as part of a normal query. There is no support for break-the-glass (BTG) functionality.

A subject of care who does not opt in “falls back” to care processes unsupported by the HIE (even though PHI is collected about them and saved to the SHR).

All ya gotta do is:

* At the CR, associate a Boolean attribute (a flag) with the enterprise client ID (ECID), which indicates if the client has opted in.
* At the CR, provide a way to set and clear this flag. This could be an administrative maintenance application (it does not need to be exposed to POS applications).
* At the IL, support inbound queries with a BTG flag and BTG reason; save the BTG flag and BTG reason to the ATNA log.
* At the IL, for each query for PHI, check the ECID’s flag and the inbound query’s BTG flag; if not opted in and BTG != TRUE, return exception; if opted in or BTG = TRUE, return requested content.
* At the POS, support:
	+ electronic capture of BTG reason and (re)execution of HIE queries as BTG queries with local electronic audit logging regarding the BTG event.
	+ education of clinician users regarding BTG and its implications
	+ education of subjects regarding their privacy rights and the implications of providing consent to disclose
	+ capture (paper-based or electronic), filing and maintenance of subject’s disclosure consent directive
	+ communication of subject’s consent directive to the CR (electronically, or via a paper-based workflow to a central CR administration).

### 5. Implied consent; segmented disclosure; support BTG

POS software modification is needed to support BTG and coding confidentiality of PHI by segment/section. Detailed electronic consent directive capture/management is needed. Sophisticated SAML and XACML services needed at HIE level. Subject and provider education needed re: privacy options.

This option is the Cadillac. As with options 1 & 2, this option assumes implied consent to 100% sharing with 100% of the authenticated HIE system users. Break-the-glass (BTG) is supported. Unlike the other options discussed so far, a subject of care may *selectively* opt out of sharing their PHI. This selectivity may apply along a number of axes including masking PHI based on the query submitter’s role (RBAC), by facility or by data segment within a clinical document.[[9]](#footnote-9) PHI that has been selectively “masked” is not returned as part of a normal query. A POS may, however, resubmit the query as a BTG query and this will override the subject’s consent directive and return all content.

The functionality in this section is very much in line with the US health interoperability group’s Data Segmentation for Privacy (DS4P) initiative ([http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage](http://wiki.siframework.org/Data%2BSegmentation%2Bfor%2BPrivacy%2BHomepage)). It leverages HL7’s and IHE’s recent work in this area and is the subject of a number of pilot projects, including one at Indiana University which leverages the Indiana HIE. Results of this IU pilot were recently reported.[[10]](#footnote-10)

One of the IU pilot participants, a physician, noted that in the face of segmented disclosure “I would inform my patients that I intended to “break the glass” (i.e., override their restrictions on EHR access, should any have been invoked) at the beginning of every visit, when I routinely perused my patients’ electronic and paper records. I have to know all there is to know about each patient, and I don’t know what I don’t know, or what’s important and relevant to that day’s care, without full access to my patients’ records. If a patient were uncomfortable with my “breaking the glass” for each visit, I would transfer his or her primary care to another physician willing to provide care without full EHR access, if I could find one.”[[11]](#footnote-11) This view (and action) seemed to be shared by a majority of physicians in the study. This should not be taken as indicative of physician preferences in the face of segmented masking, but rather as generally indicative of physician preferences in the face of patient masking of PHI.

All ya gotta do is:

* At the IL, implement a Consent Directive Management Service (CDMS).
* At the CDMS, maintain an XACML expression of a subject’s consent directive keyed by their ECID and any other segmentation identifiers (e.g. role, EPID, ELID, diagnosis code, confidentiality code, etc.).
* At the SHR, maintain content coding at the document, section and/or data element level consistent with consent directive segmentation (e.g. confidentiality codes)
* At the IL, support inbound queries with a BTG flag and BTG reason; save the BTG flag and BTG reason to the ATNA log.
* At the IL, for each query for PHI where BTG flag not set, check the CDMS for consent directives and apply XACML-based masks against the inbound query’s result set before returning the masked results; if the BTG flag is set, return all requested content with no masking.
* At the POS, support:
	+ electronic capture of BTG reason and (re)execution of HIE queries as BTG queries with local electronic audit logging regarding the BTG event.
	+ education of clinician users regarding BTG and its implications
	+ education of subjects regarding their privacy rights and the implications of fully or partially withdrawing consent to disclose
	+ capture (paper-based or electronic), filing and maintenance of subject’s disclosure consent directive
	+ communication of subject’s consent directive to the HIE (electronically, or via a paper-based workflow to a central CR administration).

# Technical Design

## Design overview

The proposed design is option #1 from the previous section. This design minimizes the technical and sociotechnical barriers to supporting privacy in OpenHIE. Alterations will be needed to three workflows:

1. Update client demographics
2. Query for client demographics
3. Query for health information.

Even in the face of making only minor changes to OpenHIE’s existing workflows, however, a fundamental moral and ethical capability will be enabled: OpenHIE will operationalize and respect a client’s ability to exert their right of privacy regarding their PHI.

Although it is expected (and recommended) that OpenHIE be operated using an opt-out model of consent, with the recommended workflow changes, the system could also be configured to support an opt-in model.

For the implementing jurisdiction, the following patient privacy policy structure is recommended:

There is a **deemed consent** for a subjects PHI’s to be **collected and disclosed** for **health care** purposes with **all providers of care**.

## Related IHE profiles

## OpenHIE workflow implications

1. 2013 COACH Guidelines for the Protection of Health Information (<http://www.coachorg.com/en/practices/Privacy_Security_Guidelines_Series.asp>) ; hereafter: COACH Guidelines [↑](#footnote-ref-1)
2. ISO 7498-2 [↑](#footnote-ref-2)
3. COACH Guidelines [↑](#footnote-ref-3)
4. Implied consent is when the actions or inactions of an individual can reasonably be taken as indicating their voluntary agreement to information sharing. [↑](#footnote-ref-4)
5. There are nuanced definitions of consent which include: implied, deemed, express/explicit, and no-consent. For purposes of this discussion document, no-consent, deemed and implied consent will all be treated as “opt-out” models and express/explicit consent will be treated as an “opt-in” model. As a convenient misdemeanor, this document will refer to all opt-out models as *implied consent*. [↑](#footnote-ref-5)
6. The number of subjects who choose to invoke “opt out” consent directives is typically low, when expressed as a proportion of the overall population. As an indicative example, in the province of Manitoba, Canada (population 1.3M) the number of *disclosure directive* (opt-out) subjects was 28 (as of September, 2012 – 2 years after the go-live of the provincial “eChart” system). <http://www.canhealth.com/sep12.html#12sepstory3> [↑](#footnote-ref-6)
7. ISO 31000 [↑](#footnote-ref-7)
8. It is recommended that OpenHIE consider adopting use of the **PD1-12 Protection Indicator** element, which may be saved as part of a PIX transaction and retrieved via a PDQ transaction [↑](#footnote-ref-8)
9. It is not possible, using current technology, to selectively mask “free text” content. In the face of this limitation, some have advocated for a “fail closed” scenario that would redact *all* free text in the face of consent directives. [↑](#footnote-ref-9)
10. Journal of General Internal Medicine, Volume 30, Issue 1 Supplement, January 2015 (8 articles) [↑](#footnote-ref-10)
11. Kelly Caine and William Tierney, *Point and Counterpoint: Patient Control of Access to Data in Their Electronic Health Records*, JGIM Vol 30, Issue 1 Supplement, Jan 2015 [↑](#footnote-ref-11)