AHCCCS

Arizona Medical Information Exchange AMIE

Manage Consent Directives

Use Case and Requirements Documentation Release 1

July 23, 2009

List of Figures

Revision History

Version #	Date Published	Description of Change	Name of Author
1.0	02/12/2009	Initial draft	Pat Rennert
1.1	02/23/2009	Extended Draft	Lupita Figueroa
1.2	07/22/2009	Added requirements	Lupita Figueroa
1.3	07/23/2009	Updated after review with business team. Added additional requirements. Reworded some requirements.	Lupita Figueroa

1 Project Description

The Health Information Exchange Electronic Health Record (HIeHR) Utility Project, under a Federal Medicaid Transformation Grant, will develop and implement a statewide, secure, online Health Information Exchange (HIE) and Electronic Health Record (EHR) system. AHCCCS was awarded the Medicaid Transformation Grant on January 25, 2007 to develop and implement a web-based health information exchange (HIE) utility to give all Medicaid providers instant access to patients' health records at the point of service. The Federal funds have been used to support the planning, design, development, testing, implementation, and evaluation of the AHCCCS Health Information Exchange and Electronic Health Record (HIeHR) Utility.

Phase 1, which began as a proof of concept in the Fall of 2008, is a federated health information exchange (HIE) with a secure web-based viewer through which authorized AHCCCS registered healthcare providers will be able to match patients, locate relevant information, and view individual documents. This exchange will include:

1. *Hospital Discharge Summaries*

2. *Laboratory Test Results*

3. *Medication History*

The exchange has been rebranded Arizona Medical Information Exchange (AMIE) and has been successfully deployed as a proof of concept to over 40 physicians and support staff in three major hospital systems and several affiliated practices. The proof of concept phase was to close out and provider feedback data for analysis at the end of December, 2008. Due to the value various clinicians, particularly in the emergency department setting, found in the AMIE application, it was decided to continue running the exchange until September, 2009.

The AHCCCS behavioral health program administered by the Department of Health Services took an interest in engaging the Regional Behavioral Health Authority (RBHA) clinics to utilize AMIE in order for their providers to benefit from the efficiency of obtaining medical records that AMIE provides. This entailed training and introducing over 50 additional users to the exchange and expanded its use geographically beyond the Phoenix Metro area.

Since the concept of AMIE was validated as a user friendly, intuitive application that generally provided critical health care information at the point of care and found to be a valuable tool in health care delivery, the application has expanded beyond the “proof of concept” phase.

2 Introduction

1.1 Background

One of the fundamental challenges all HIEs face is that of establishing policies around consumer consent directives and developing the technology to support those directives. Some policy decisions are too difficult or expensive to implement. Additionally, many states differ in their regulations for managing consent directives.

In order to make informed decisions regarding the adoption of a patient consent policy and model, the AMIE team conducted research on the following:

- Reviewed HITSP and CCHIT guidelines for messaging and standards for implementing a solution for managing consent directives.
- Reviewed Arizona health-e connection (AZHEC) guide white paper which listed issues and options for consent models in Arizona. This white paper reviewed the consent models available and their barriers to implementation. The consent models analyzed consisted of Opt-in, Opt-Out, Notice Only, and Combination.
- Reviewed the National Committee on Vital and Health Statistics recommendations, the 21 state survey conducted by Healthcare Information and Management Systems Society for best practices, and the Health Information Security and Privacy Collaborative survey of eleven states.
- Reviewed ARHQ Privacy and Security Assessment of Variation Toolkit
- Analyzed consent models adopted by other Health Information Exchanges across the nation

Kristen Rosati, in “Consumer Consent for Health Information Exchange: An Exploration of Options for Arizona’s HIEs”, a white paper for AzHEC describes Arizona Law regarding consent. Among the requirements she lists are the following:

- Arizona law does not require consumer consent to exchange health information for treatment purposes.
- Arizona law generally does not require consumer consent for providers to exchange health information for a variety of purposes, such as getting paid for the treatment they provide, for various business functions called “health care operations” (such as quality assurance activities), for public health purposes, and for research where an institutional review board has reviewed the research and approved doing the research without consent (if there is sufficient privacy protection in place).
- In reference to HIPAA, it is stated that disclosures for treatment, payment, “health care operations”, public health purposes, and research, is permitted without consumer consent or authorization.

In particular, she mentions that the only restrictions that apply to exchanging data involve the following scenarios:

- Genetic testing information exchanged with Health Plans without patient's advance consent.

- Drug and alcohol treatment information that originates from providers that have federally-assisted substance abuse treatment programs should not be exchanged.

Based on this research, the AMIE team recommended that they should initially adopt an opt-out consent model since it would meet current requirements for exchanging data in Arizona. It is the intent that this model would evolve over time as new regulations are put into place and health information technology standards for consent are adopted by vendors.

1.2 Description

This manage consent directive use case will focus on expanding the healthcare providers' current role of Notification of Privacy Practices to include informing patients about AMIE and present them with the opportunity to opt-out of allowing their medical information to be shared. It will define the additional steps required that will affect work flow at the point of patient registration, potential issues, and how this process may be handled when interfacing with other states' health information exchanges. Also, it will illustrate the role AMIE will play in storing and enforcing these consent directives.

1.3 Scope

This use case will include the following scenarios:

1. Capture consent directive to opt-out or reverse decision and opt-in
2. Override consent directive (break the glass)

1.4 Constraints

1. There is not a 100% reliable method for uniquely identifying patients across organizations which limits the reliability of a global opt-in or opt-out throughout the AMIE system.
2. The consent models for NHIN or other HIEs and messaging standards are not yet fully developed.
3. Consent directive level of granularity is constrained by current technology, healthcare standards and implementation costs.
4. Consent directives cannot be captured and maintained by patients at this time, since it would require AMIE to provide a patient user provisioning process just for capturing consent directives.
5. Timing becomes an issue if at the time of registration the patient has not been seen by any data providers that would initiate an account in AMIE.

2 AMIE Current and Proposed Consent Model

2.1 AMIE Consent Model Description (AS-IS)

For the proof of concept, AMIE delegated patient consent management to the Data providers with the exception of providing the technology to support their consent policy requirements. AMIE informed data providers that the clinical information would be used only for treatment purposes and by a limited number of users. Data providers were given the responsibility to inform the patient that their information will be available through AMIE for providers outside of that setting to view for treatment purposes. It was requested that they notify AMIE if a patient requested to opt-out of making their clinical records available. Various mechanisms were presented as to how to facilitate this and each data provider took a different approach to clinical information disclosure. Some of the non-standardized approaches taken are listed below:

MIHS

- MIHS automatically flags its employee records with record release restrictions. Also, they manually flag patient records that cannot be disclosed according to HIPAA guidelines per patient election and records that contain clinical information that cannot be disclosed due to legal restrictions.

Sonora Quest

- Sonora Quest does not have a mechanism to support an electronic patient opt-out option nor do they inform patients that information is disclosed through AMIE. Their approach was to apply a filter to sensitive data and withhold based on that. Sensitive data as defined by AMIE consisted of lab orders containing genetic, STD, HIV, or drug abuse related tests.

Banner Health

- Banner uses a NINP (No Information No Publication) flag to filter out patient records for patient. In particular, Banner sends only data from facilities that do not offer behavioral health patient process. Banner current process poses the problem of not providing a mechanism to change a patient’s election from opt-out to opt-in. In fact, in some cases AMIE does not even know that the patient records exist, therefore putting a constraint on the future implementation of a break the glass scenario.

SJHMC

- St. Joseph’s Hospital and Medical Center, is the only data provider that actively informs the patient of AMIE and allows the patient to choose to have their information flagged and withheld from the RLS.

The expansion of AMIE to include other data consumers in addition to the AMIE viewer and new types of data providers and data consumers brings new challenges that the current architecture cannot surpass.

Due to the variation in consent management across all data providers and planned expansion of data providers/consumers/users, the AMIE team has determined that a more comprehensive and standardized consent process in which *all* patients are informed at the point of care needs to be developed and adhered to by all data providers.

2.2 AMIE Consent Model Description (TO-BE)

The proposed policy provides consumers with the right to "opt-out" of having their health information available through AMIE for treatment purposes only. By default, patient will be placed in an opt-in status until the patient chooses to opt-out. If opt-out status is chosen, none of a patient's information will be available through AMIE. Data shared by data providers will be indexed in the RLS in order to be available in an emergency. AMIE will provide online tools to manage patient consent directives by the facility where the patient expresses their desire to opt-out. Below are some policy assumptions for the proposed TO-BE consent model.

AMIE consent policy assumptions

1. **What are the different patient entry privacy statuses that AMIE will support?**

Every AMIE patient entry will be in one of these statuses:

- Opt-in by default– Patient may not have been previously notified of AMIE and therefore has not had a chance to opt-out. Access to data would be used only for the purposes of treatment by authorized AMIE participants.
- Opt-out by Election (with emergency override) – Patient has been presented with information about AMIE and has decided to opt-out of allowing access to their data for any reason, with a "break the glass" exception.

2. **Will data providers notify past patients of their default opt-in status?**

No, data providers will not be required notify past patients of their default opt-in state. Patients will be informed of their default opt-in state only if they return to visit any AMIE active healthcare provider. At that time they will be given the opportunity to opt-out.

Providers may simply present the patients with the notification that their information will be made available in a health information exchange, unless they specifically choose to opt out.

3. **Who will capture and manage patient's consent directive?**

AMIE authorized Healthcare providers and/or their staff will be responsible for capturing patient consent directives during patient encounters at their facility. The provider or staff will electronically submit this request to AMIE through the manage consent function.

4. **Are opt-outs/opt-ins data provider specific or will they apply to the entire AMIE system?**

Opt-outs/opt-ins patient will apply throughout the entire system regardless of where the consent directive originated and the origin of all patient records available. If a patient opt-outs, he/she opts out of allowing access to all his/her data. Also, if a patient opt-out at Hospital A, then opts-in at Hospital B, both the data of Hospital A and Hospital B will be made accessible through AMIE.

5. **Who will be able to access patient records and for what purpose?**

Only authorized AMIE participating providers will be allowed access for treatment purposes only.

6. **What data may be accessed by those being granted access?**

Lab Results, except genetic, STD, drug substance abuse, and HIV related tests.
All Clinical Documents, except those manually flagged by data provider as sensitive due to health information or legal reasons. All Medication History only for AHCCCS patients.

7. **Is AMIE going to exchange records with other Health Information Exchanges?**

Not at this time.

8. **After patient opts-in, is data during opt-out period going to be made available?**

Yes, all data regardless of the time when it originated will be made available if patient opts-in. The only exception is if data provider does not want AMIE to enforce consent and they want to do it at their interface.

9. **Will AMIE support a break the glass scenario, in which patient consent directive may be overridden?**

Yes, consent directives may be overridden in case of emergency, professional judgment, public safety, and third party safety. The reason will always be stated and logged in the audit trail. AMIE security officer and patient or patient's representative will be notified ASAP.

Below is a list of the HL7 valid coded reasons,

Emergency - The patient is unable to provide consent, but the provider determines they have an urgent healthcare related reason to access the record. (e.g. Patient presents in unconscious, delirious or otherwise uncommunicative state.)

Professional Judgment - The patient, while able to give consent, has not. However the provider believes it is in the patient's interest to access the record without patient consent.

Public Safety - The patient, while able to give consent, has not. However, the provider believes that access to masked patient information is justified because of concerns related to public safety.

Third Party Safety - The patient, while able to give consent, has not. However, the provider believes that access to masked patient information is justified because of concerns related to the health and safety of one or more third parties.

"Emergency" as defined by Title 20-2801:

"Emergency services" means health care services that are provided to an enrollee in a licensed hospital emergency facility by a provider after the recent onset of a medical condition that manifests itself by symptoms of sufficient severity that the absence of immediate medical attention could reasonably be expected to result in any of the following:
(a) Serious jeopardy to the patient's health.
(b) Serious impairment to bodily functions.
(c) Serious dysfunction of any bodily organ or part.

10. **Will AMIE locate records if patient revokes consent once they had been disclosed during an opt-in period?**

    No, AMIE will not locate records at different data consumers to revoke consent. Current architecture allows records to be kept only at their originating location. Copies of these records will not be kept in any other place. Therefore, only access to these records will be revoked.

    In the event, copies are distributed to other locations, it will be AMIE's policy that these copies are not served or published as available by other locations.

11. **Will AMIE notify data consumers of patient's consent directive updates, such as changes from opt-in to opt-out?**
    No.

12. **How will health care provider capture consent if no account yet exists?**

    Assumption is that if no account exists on first encounter with a participating entity, one will have to be established prior to records being created for services rendered. This will be done through the AMIE consent management function.

13. **Will clinicians continue to be the primary users of AMIE and manage consent directive information?**

    Assumption is that support staff will be responsible for entering information to create new patient entry or capture consent directive. In a hospital, almost certainly it will be support staff. In a clinic setting, clinicians may perform this task. In either scenario, it could be both.

14. **Will an account need to be created for patients who are opted in by default?**

    No.

4 Stakeholders

Stakeholder	**Working Definition**	**Stakeholder Value**
Patients (consumers)	Individuals presenting for care	-Need to know that their PHI will be available in an electronic format -Will be educated as to the value of their PHI being available instantly in an HIE
Physicians	Primary Care physicians and clinicians practicing in a clinical setting	-Inform and reinforce concept of *minimum necessary* disclosure of PHI -Will be informed in how to avoid and recognize a security breach
Clinical Staff	Includes front office staff who are responsible for scheduling, the preparation of patient records, gathering information prior to and after a patient visit. Back office staff that validates records	-Will be prepared to provide consent information and answer questions -Will be provided with FAQs to help facilitate this -

	obtained from the Viewer and assimilates other data in preparation for physician treatment.	
Health Plans	Insurers & third party administrators who provide healthcare benefits to insured members.	-
Labs		
Hospitals		
Behavioral Health		
NHIN and other HIEs	National Health Information Network	
Research Organizations		
Government Agencies (AHCCCS, SSA)		

5 Assumptions

Assumptions are necessary to establish a starting point for this use case. Either certain events need to have occurred or other requirements must be in effect for this use case to be effective. These are listed to generate a common understanding of the starting point. As this use case progresses, these assumptions may change as each user group may identify new events that must first be considered. The starting assumptions are:

- All users are authorized user of the AMIE Utility Tool.
- All users have completed training and acknowledge that they are bound by the Provider Participation Agreement privacy and security policies.
- The patient has visited and received treatment by participating facilities.

6 Obstacles / Issues to Implement Use Case

Data provider training Issues
Data provider workflow integration issues
Creating Required Forms to support process

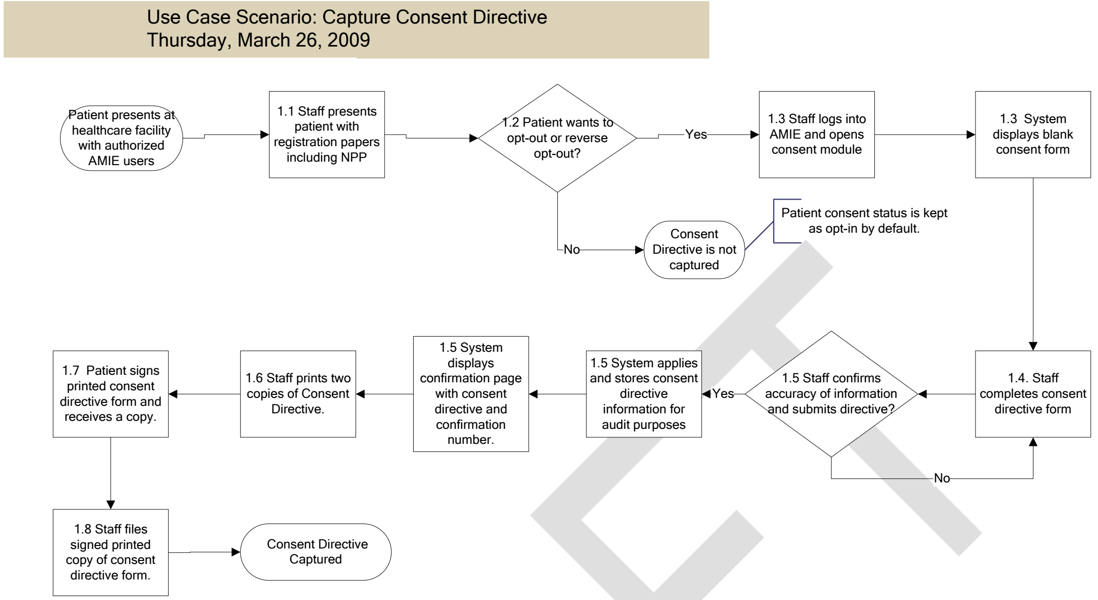
3 Perspectives & Scenarios

3.1 Perspectives

Clinician
System – AMIE
Healthcare Staff
Security Officers

3.2 Scenarios

3.2.1 Capture Consent Directive


Use Case Scenario: Capture Consent Directive
Thursday, March 26, 2009

Patient presents at healthcare facility with authorized AMIE users
1.1 Staff presents patient with registration papers including NPP
1.2 Patient wants to opt-out or reverse opt-out?
Yes
1.3 Staff logs into AMIE and opens consent module
1.3 System displays blank consent form
No
Consent Directive is not captured
Patient consent status is kept as opt-in by default.
1.4. Staff completes consent directive form
1.5 Staff confirms accuracy of information and submits directive?
No
Yes
1.5 System applies and stores consent directive information for audit purposes
1.5 System displays confirmation page with consent directive and confirmation number.
1.6 Staff prints two copies of Consent Directive.
1.7 Patient signs printed consent directive form and receives a copy.
1.8 Staff files signed printed copy of consent directive form.
Consent Directive Captured

Brief Description:	Healthcare staff captures patient's new or updated consent directive to opt-out, opt-in or takes no action to change their patient's default opt-in status.
Business Trigger (what initiates the 1st Actor Action):	Patient visits one of the AMIE authorized health care provider/users and decides to opt-out or opt-in by election.
Pre-Conditions:	Healthcare staff must have sufficient permissions to update/create consent directives on behalf of the patient.

Basic Flow:

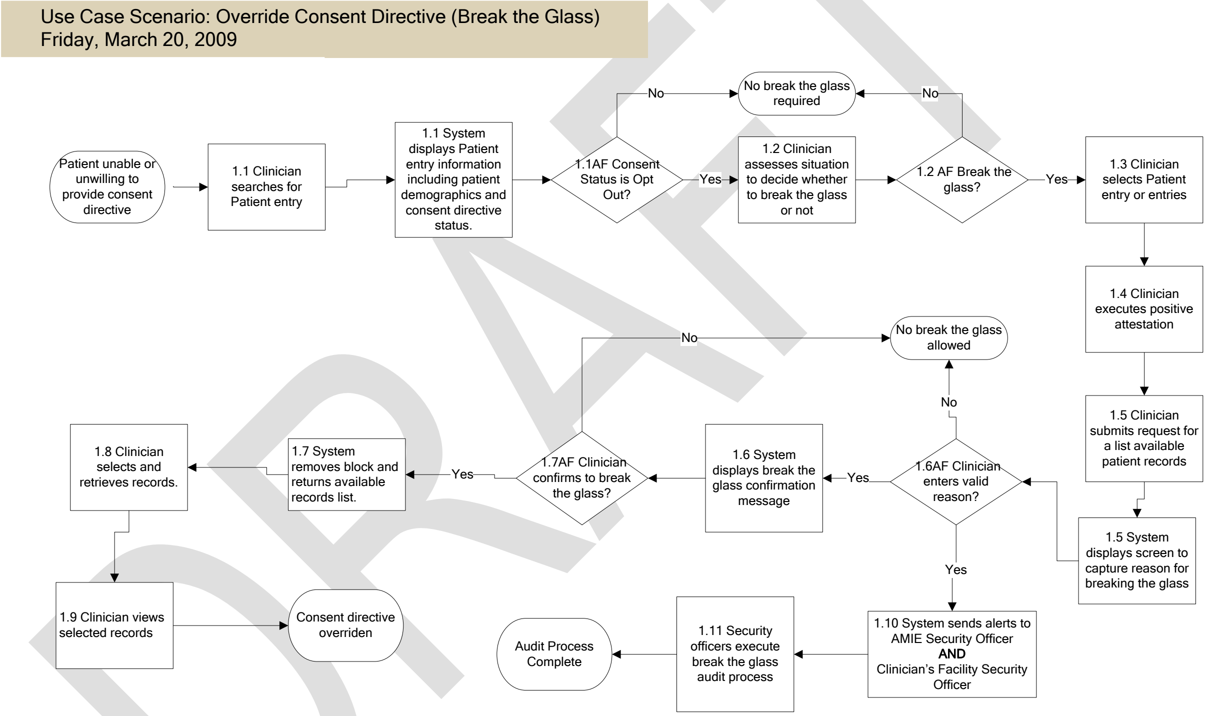
Code	**Event / Actor Action**	**System Response**	**Notes / Alt. Flow**
1.1	Staff presents patient with registration paperwork including Notice of Privacy Practices.	None	Assumption: Provider may use
1.2	Patient decides to opt-out or reverse its opt-out election. .	None	**AF:** If patient decides to keep its patient entry status as opt-in by default. Staff will take no further action and flow will terminate.
1.3	Staff logs into AMIE system and	System displays	

	opens consent module.	blank consent directive form	
1.4	Staff completes consent directive form by entering required information.	System displays consent directive review page with completed form for verification of accuracy.	
1.5	Staff confirms accuracy of information and submits consent directive.	System applies and stores consent directive information for audit purposes. System displays confirmation page with consent directive information and confirmation number.	Confirmation number is a unique id assigned by the system to uniquely identify the transaction. Confirmation page displays the complete consent directive with all information entered by user, submission information and legal agreement. AF: Staff does not confirm accuracy of consent directive. Staff should be given the option to correct errors or cancel.
1.5	Staff prints two copies of consent directives.	System prints a printer friendly version of the consent directives.	Consent directive must contain the following: • Patient demographics • Patient's legal representative if required. • Consent directive details • Submission Information
1.6	Patient signs printed consent directive form and receives a copy.	None	Healthcare provider files a copy of printed consent directive signed by patient as part of patient medical record. Alternatively, Healthcare provider may scan the

			document and file a copy of this form in an electronic medical record.
1.8	Staff files the signed printed copy of consent directive.	None	The healthcare provider must keep a copy of the printed AMIE consent directive form signed by the patient for their records.

Pot Condition:	Consent directive has been captured

3.2.2 Override Consent Directive (Break the Glass)


Use Case Scenario: Override Consent Directive (Break the Glass)
Friday, March 20, 2009

Patient unable or unwilling to provide consent directive
1.1 Clinician searches for Patient entry
1.1 System displays Patient entry information including patient demographics and consent directive status.
1.1AF Consent Status is Opt Out?
No
No break the glass required
No
Yes
1.2 Clinician assesses situation to decide whether to break the glass or not
1.2 AF Break the glass?
Yes
1.3 Clinician selects Patient entry or entries
1.4 Clinician executes positive attestation
1.5 Clinician submits request for a list available patient records
1.5 System displays screen to capture reason for breaking the glass
No
No break the glass allowed
No
1.6AF Clinician enters valid reason?
Yes
1.6 System displays break the glass confirmation message
1.7AF Clinician confirms to break the glass?
Yes
1.7 System removes block and returns available records list.
1.8 Clinician selects and retrieves records.
1.9 Clinician views selected records
Consent directive overriden
Yes
1.10 System sends alerts to AMIE Security Officer AND Clinician's Facility Security Officer
1.11 Security officers execute break the glass audit process
Audit Process Complete

Brief Description:	Healthcare staff overrides patient's consent directive in order to retrieve patient records in case of emergency or other permitted reasons as defined by AMIE policy.
Business Trigger (what initiates the 1st Actor Action):	Patient visits AMIE authorized health care provider/user and is unable or unwilling to provide consent directive. (e.g. Patient presents in unconscious, delirious or otherwise uncommunicative state.)
Pre-Conditions:	Clinician must have sufficient permissions to override consent directives (break the glass) to access patient records. Clinicians logs into AMIE viewer with appropriate credentials.

Basic Flow:

Code	**Event / Actor Action**	**System Response**	**Notes / Alt. Flow**
1.1	Clinician searches for patient entry	System returns patient entry information which shows consent directive status. Patient entry search results will display demographic based information: AHCCCS ID (if applicable), Last Name, First Name, Date of Birth, Gender, SSN (4) (last four digits of Social Security Number), Address, City, State, and Zip Code.	All patient entries will be listed regardless whether patient has opted-in or opted-out, but clinicians should NOT be able to retrieve patient entries from patients who opted-out without asserting that they want to break the glass. Only patient entries that have associated medical records available should be displayed. **AF:** if patient entry is not in an opt-out status, then no break the glass is required and flow terminates.
1.2	Clinician assesses situation to decide if it meets criteria for breaking the glass or not.		
1.3	Clinician selects Patient entry or entries		
1.4	Clinician executes positive attestation	System records clinician relationship with the patient was asserted.	
1.5	Clinician submits request for a list available patient records	System displays screen to capture reason for breaking the glass. System will list valid reasons for breaking the glass, as well as input space for physician to enter incident notes. Valid reasons for breaking the glass may include emergency, professional judgment, public safety and third party safety.	Screen to capture reason for breaking the glass must include the following: • Permitted Criteria for breaking the glass • Notice that alert will be generated and sent to AMIE and healthcare facility security officers • Reason List • A place to enter Incident notes

1.6	Clinician selects reason(s) for breaking the glass and enters incident notes.	System displays confirmation message for breaking the glass.	Clinician's confirmation for breaking the glass, reason for breaking the glass, and patient relationship attestation are all pre-conditions to removing block on patient entry. For each patient entry selected by clinician all this pre-conditions need to be met. AF: if clinician does not confirm to break the glass, he/she will not be permitted to break the glass and flow terminates.
1.7	Clinician confirms to break the glass.	System generates and sends alert to AMIE and healthcare facility security officers. System removes block for retrieving patient entry available records information and returns available record list.	
1.8	Clinician selects and retrieves records.		
1.9	Clinician views selected records		
1.10	System sends alerts to AMIE Security Officer and Clinician's Facility Security Officer		Alert must be generated as soon as clinician breaks the glass and gets access to list of patient records. Alert must include the following information: Date of Incident Patient Index ID Consent Directive ID Consent Directive Status
1.11	Security officers execute break the glass audit process		Officers will be responsible of the following: Validation that the incident

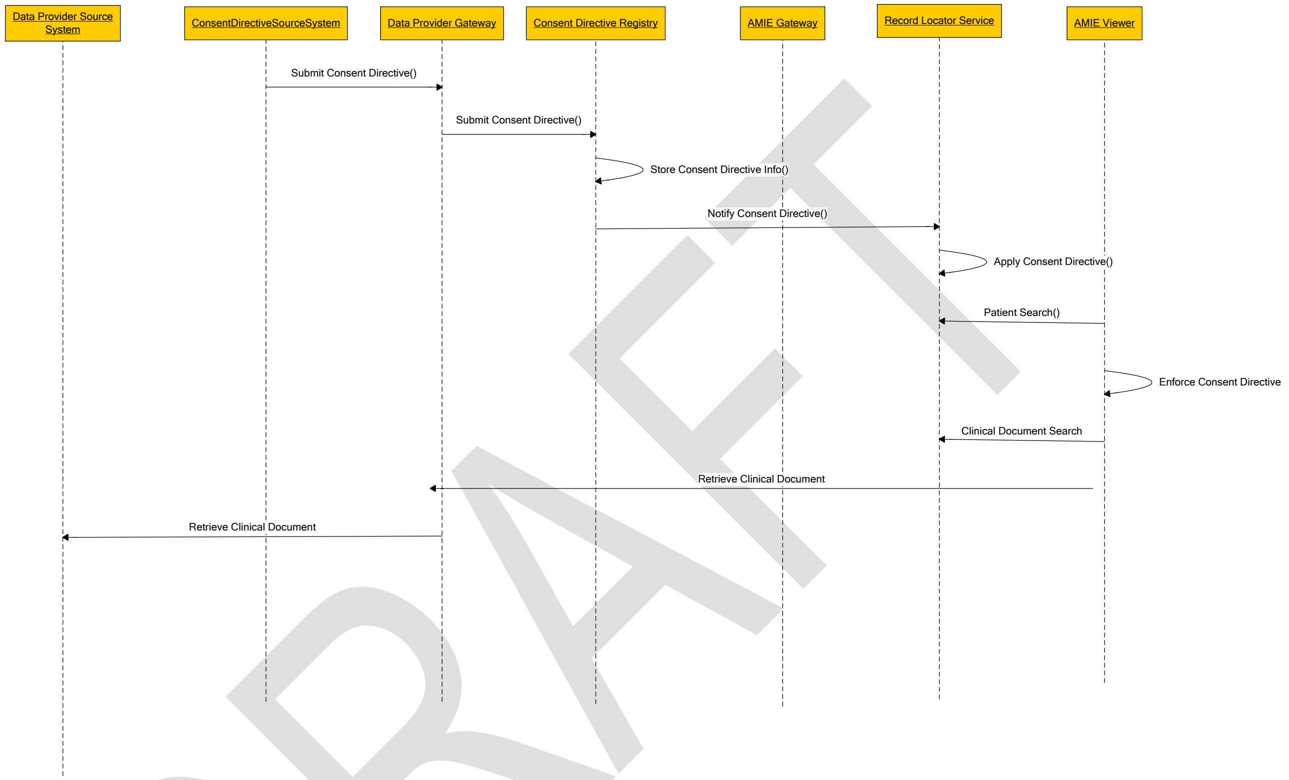
			met the criteria for breaking the glass Notifying the patient as soon as possible that the break the glass feature was use on their records.

Post Condition:	Consent Directive Overridden – Clinician has ability to see view all records available for a patient with opt-out status.

4 Requirements

Req. No.	Requirement
1.1	The system shall provide a web based application that enables only authorized users based on their role to capture a patient's consent directive.
1.2	The system shall provide the ability to set up a specialized role with the approriate permission to capture and submit a consent directives.
1.3	The system shall provide the ability to set up a specialized role with the approriate permission to break the glass.
1.4	The system shall provide the ability for a patient to opt-out, so that all of their clinical documents available through AMIE have restricted access.
1.5	The system shall provide the ability for a patient to opt-out, so that only clinical documents from a specific data provider have restricted access.
1.6	The system shall provide the ability for a patient to revoke its previous consent directive election.
1.7	The system shall maintain a chronological history of all consent directives submissions.
1.8	The system shall provide the ability to capture patient demographics, patient legal representative, and consent directive election when capturing consent directive information.
1.9	The system shall provide the ability to preview consent directive information before submission.
1.10	The system shall maintain a consent directive registry that maintains a listing of all consent directives
1.11	The system shall provide a matching algorithm in order to apply consent directives to patient records in the master pateint index.
1.12	The system shall provide the ability for role appropriate AMIE viewer users to override a patient's consent directive by breaking-the-glass.
1.13	The system shall prevent a user from breaking the glass, if they do not enter a reason for breaking-the-glass.
1.14	The system shall provide the ability to configure the break-the-glass reason list.
1.15	The system shall provide the ability to maintain a list of organizations' security officers/contacts.
1.16	The system shall send an email alert to the user's organization security officer for each break-the-glass event. The email alert must contain the following information: date of incident, patient ID, and ID of consent directive that
1.17	The system shall provide the ability to perform a patient search on all patient records, regardless of patient's consent directive.
1.18	The system shall display patient demographics and consent directive election within the patient search results.
1.19	The system shall prevent a user to view the list of clinical documents available for patients with an opt-out status.
1.20	The system shall provide the ability to print consent directive before submission for patient review and signature.
1.21	The system shall provide an interface for data provider source systems to submit consent directives to the consent registry.
1.22	The system shall provide the ability to notify AMIE ops security personnel of a change in patent's consent status.
1.23	The system shall provide the ability to notify AMIE ops security personnel after a break the glass incident.
1.24	The system shall provide a configurable disclaimer notification that they are responsible for identifying the patient and they will retain signed consent directive copy upon submission.
1.25	The system shall enforce patient consent directive at the point where the user tries to query for the list of available clinical documents for specific patient(s)
1.26	The system must use the XACML standard for communicating consent directives.
1.27	The system must provide a SOAP inteface to which consent directives may be submitted by data provider's

5 Upon Consent Directive Submission Process


Data Provider Source System
ConsentDirectiveSourceSystem
Data Provider Gateway
Consent Directive Registry
AMIE Gateway
Record Locator Service
AMIE Viewer
Submit Consent Directive()
Submit Consent Directive()
Store Consent Directive Info()
Notify Consent Directive()
Apply Consent Directive()
Patient Search()
Enforce Consent Directive
Clinical Document Search
Retrieve Clinical Document
Retrieve Clinical Document

6 Approval

APPROVED BY:

______________________________ ______________________

Date

7 Glossary

Data Consumer – A organization’s system that makes use of clinical data.

8 Supporting Information and References

8.1 How Other States are Handling

State - HIE	CalRHIO - HIE	New Mexico	Wisconsin	Indiana
Standard	Markle - Connecting For Health Common Framework			
Choice Not to Have Information Included in the RLS	All individuals may choose not to have information about them included in or made available through the RLS.			
Who manages patient's choice to opt or opt out	Participant, being clinic or hospital. Participants shall develop and implement appropriate mechanisms to remove information about an individual from the RLS if the individual chooses to have such information excluded from the			

	RLS.			
Revocation	An individual who has chosen not to make information concerning him or her available through the RLS subsequently may be included in the RLS only if the individual revokes his or her decision or subsequently chooses to renew participation in the RLS.			
Documentation	Each Participant shall document and maintain documentation of all patients' decisions not to have information about them included in the RLS.			
Participant Choice	Participants shall establish reasonable and appropriate processes to enable the exercise of a patient's choice not to have information about him or her included in the RLS. Each Participant retains the authority to decide whether and when to obtain patient consent prior to making information available through the RLS.			
Accounting of Disclosures	Each Participant disclosing health information through CalRHIO shall work towards implementing a system to document the purposes for which such disclosures			

	are made, as provided by the requesting institution, and any other information that may be necessary for compliance with the HIPAA Privacy Rule's accounting of disclosures requirement. Each Participant is responsible for ensuring its compliance with such requirement and may choose to provide individuals with more information in the accounting than is required. Each requesting institution shall provide information required for the disclosing institution to meet its obligations under the HIPAA Privacy Rule's accounting of disclosures requirement.			
Audit Logs	Participants **and** CalRHIO shall consider and work towards maintaining an audit log documenting which Participants posted and accessed the information about an individual through the RLS and when such information was posted and accessed. Participants and CalRHIO shall consider and work towards implementing a			

	system wherein, upon request, patients have a means of seeing who has posted and who has accessed information about them through the RLS and when such information was accessed.			
Authentication	Each Participant shall follow uniform minimum authentication requirements for verifying and authenticating those within their institutions who shall have access to, as well as other Participants who request access to, information through the CalRHIO and/or the RLS.			
Access	Each Participant should have a formal process through which information in the RLS can be requested by a patient or on a patient's behalf. Participants and CalRHIO shall consider and work towards providing patients direct access to the information contained in the RLS that is about them.			
Information Subject to Special Protection	Some health information may be subject to special protection under federal, state, and/or local laws and regulations (e.g., substance abuse, mental			

	health, and HIV). Each Participant shall determine and identify what information is subject to special protection under applicable law prior to disclosing any information through CalRHIO. Each Participant is responsible for complying with such laws and regulations.			
Issues/Obstacles	Could not find			

Deleted Reference Material and Questions

There are multiple issues to address in introducing this process to the currently participating data partners.

- Training Issues - This will be a new process for them to train on and be prepared to answer patient's questions. It will need to be determined how much will be expected of them in teaching the patient about the exchange or if they will simply provide the documentation and let the patient make their own determinations.
- Creation of New Documentation - Creation of consent form and policy for validating patients' identity.
- Will need to define a policy that does not allow patients to change their minds, or allow patients to reverse their decision, or create a default policy of including their data in the RLS if a signed consent form to opt out is not received. (See excerpt below from IHE Wiki for possible policies)
- How much do patients know now how do we inform them?
- Language will need to be developed around informing the patient of the viewer and what their options are and format in which it will be presented.
- How much support from the AHCCCS member services department (headed by Linda Skinner) will be provided?
- Will the AHCCCS member services department want to distribute a formal announcement to their members?
- What role will the AHCCCS plans play?
- Inter-jurisdictional Portability - Consumer privacy consent laws and requirements, and consumer privacy desires and directives in one jurisdiction may not be legally applicable/enforceable in another jurisdiction
- Cross-validation and verification of conflicting consents.
- Need for Consent Directives defined to an Electronic Standard that covers how to collect, capture, transmit, modify, and reject consent directives.

Use Case – Manage Consent Directives

6.1 Possible Privacy Policies (from Basic Patient Privacy Consents (BPPC)- from the IHE Wiki)

Not all policies can be supported in an HIE environment. Policy development will need to include very specific language around defining exactly what the policies mean. Patients would need to understand that Opt-In policy does not mean that any person has access to their information and that there are well-written rules regarding the types of structural and functional roles are allowed access. Policies should be written to clearly indicate that what minimal information is provided to billing, and what allowances there are for system maintenance. It would define what recourse patients have to change their decisions to opt in or out. The following is a summary of what privacies can be supported, may possibly be supported, what are not possible:

Supportable

1. Opt-In to clinical use
2. Opt-Out of sharing outside of local event use, allowing emergency override
3. Opt-Out of sharing outside of local event use, without emergency override
4. Specific document is marked as available in emergency situations
5. Additionally allow specific research project
6. Additionally allow specific documents to be used for specific research projects
7. Limit access to functional roles (eg: healthcare) (direct care) providers
8. Limit access to structural roles (eg: organizational) (radiologist, cardiologist, billing clerk)
9. multiple policies apply to each document
10. Change the consent policy (change from opt-in to opt-out)
11. Allow direct use of the document, but not allowed to re-publish
12. when the document is published on media using XDM
13. when the document is published point-to-point using XDR
14. when the document is retrieved across communities using XCA
15. individual policy for opt-in at each clinic
16. individual policy for opt-in for a PHR choice (choosing from all possible PHRs - HIMSS 2008)

Possible - These might be possible depending on complex additional services that are not known at this time.

1. Allow access only to care providers with a direct treatment relationship
2. Spouse not allowed access (to all or specific document)
3. Parent is not allowed access (to all or specific document)
4. Restrict access to a specified care-setting
5. All accesses to the data will result in a notification of the patient (eg: email or such)
6. All accesses to the data require that a new consent be captured (eg: capture new signature)
7. when HL7 v2 or v3 messages are used. This would require further profiling of the use of confidentialityCode in those messages.
8. when DICOM is used. This would require further profiling of the use of confidentialityCode in those messages.
9. temporarly allowing a use of a document that would be not allowed by the current policies. This could be done with a new consent being registered that is soon after deprecated, but this is not very good solution.

Not Possible

1. Patient identifies individuals that have rights to their data
2. Patient identifies individuals that do not have rights to their data
3. Each access of the data must be individually authorized by the patient
4. a document with a mixture of more/less sensitive information thus needing different levels of protection

5. Notification to those that have used a document under consent that is now revoked
6. pulling back copies of documents that have been used under a consent that is now revoked

NOTES FROM PAT\

- The RLS will manage consent data utilizing HL7 messaging.
- It will be an exchange to exchange relationship of types of information patients have consented to.
- Will be conducive to partnering with the managed care plans.
- Will need to be suitable and compliant to HIPAA Confidentiality Rules until legislation changes.
- Will accommodate a “break the glass” scenario.
- Will be patient driven, they may enter the website and execute their options.
- Will be managed by the data partner on behalf of the patient or will give the patient directions on how to manage their consent via the website.
- Or, the data partner will tell the AMIE operations team and consent would be managed by the IT team.
- Have the choice to “opt out” of allowing their medical records to be available through the exchange and in doing so sign a disclaimer that they understand that their care may not be optimal due to the restricted availability of medical records in a paper format.
- Sign a consent indicating they acknowledge the benefit of the AMIE application and agree that their records should be available through the exchange.
- The patient would understand that their choice is an “all or nothing” choice, which means they can not ask to restrict release of their records in certain settings.
- The patient would understand that they may choose to opt out at some point after authorizing their records to be available on the exchange, should a diagnosis arise that would be conducive to them doing so.
- Each data partner has a consent process in place. Will they be agreeable to incorporate AMIE consent into their Notice of Privacy Practices

There are multiple issues to address in introducing this process to the currently participating data partners.

- Training Issues - This will be a new process for them to train on and be prepared to answer patient’s questions. It will need to be determined how much will be expected of them in teaching the patient about the exchange or if they will simply provide the documentation and let the patient make their own determinations.
- Creation of New Documentation - Creation of consent form and policy for validating patients’ identity.
- Will need to define a policy that does not allow patients to change their minds, or allow patients to reverse their decision, or create a default policy of including their data in the RLS if a signed consent form to opt out is not received. (See excerpt below from IHE Wiki for possible policies)
- How much do patients know now how do we inform them?
- Language will need to be developed around informing the patient of the viewer and what their options are and format in which it will be presented.
- How much support from the AHCCCS member services department (headed by Linda Skinner) will be provided?
- Will the AHCCCS member services department want to distribute a formal announcement to their members?
- What role will the AHCCCS plans play?

- Inter-jurisdictional Portability - Consumer privacy consent laws and requirements, and consumer privacy desires and directives in one jurisdiction may not be legally applicable/enforceable in another jurisdiction
- Cross-validation and verification of conflicting consents.
- Need for Consent Directives defined to an Electronic Standard that covers how to collect, capture, transmit, modify, and reject consent directives.

6.1 Possible Privacy Policies (from Basic Patient Privacy Consents (BPPC)- from the IHE Wiki)

Not all policies can be supported in an HIE environment. Policy development will need to include very specific language around defining exactly what the policies mean. Patients would need to understand that Opt-In policy does not mean that any person has access to their information and that there are well-written rules regarding the types of structural and functional roles are allowed access. Policies should be written to clearly indicate that what minimal information is provided to billing, and what allowances there are for system maintenance. It would define what recourse patients have to change their decisions to opt in or out. The following is a summary of what privacies can be supported, may possibly be supported, what are not possible:

Supportable

17. Opt-In to clinical use
18. Opt-Out of sharing outside of local event use, allowing emergency override
19. Opt-Out of sharing outside of local event use, without emergency override
20. Specific document is marked as available in emergency situations
21. Additionally allow specific research project
22. Additionally allow specific documents to be used for specific research projects
23. Limit access to functional roles (eg: healthcare) (direct care) providers
24. Limit access to structural roles (eg: organizational) (radiologist, cardiologist, billing clerk)
25. multiple policies apply to each document
26. Change the consent policy (change from opt-in to opt-out)
27. Allow direct use of the document, but not allowed to re-publish
28. when the document is published on media using XDM
29. when the document is published point-to-point using XDR
30. when the document is retrieved across communities using XCA
31. individual policy for opt-in at each clinic
32. individual policy for opt-in for a PHR choice (choosing from all possible PHRs - HIMSS 2008)

Possible - These might be possible depending on complex additional services that are not known at this time.

10. Allow access only to care providers with a direct treatment relationship
11. Spouse not allowed access (to all or specific document)
12. Parent is not allowed access (to all or specific document)
13. Restrict access to a specified care-setting
14. All accesses to the data will result in a notification of the patient (eg: email or such)
15. All accesses to the data require that a new consent be captured (eg: capture new signature)
16. when HL7 v2 or v3 messages are used. This would require further profiling of the use of confidentialityCode in those messages.
17. when DICOM is used. This would require further profiling of the use of confidentialityCode in those messages.
18. temporarily allowing a use of a document that would be not allowed by the current policies. This could be done with a new consent being registered that is soon after deprecated, but this is not very good solution.

Not Possible

7. Patient identifies individuals that have rights to their data
8. Patient identifies individuals that do not have rights to their data
9. Each access of the data must be individually authorized by the patient
10. a document with a mixture of more/less sensitive information thus needing different levels of protection
11. Notification to those that have used a document under consent that is now revoked
12. pulling back copies of documents that have been used under a consent that is now revoked

NOTES FROM PAT

- The RLS will manage consent data utilizing HL7 messaging.
- It will be an exchange to exchange relationship of types of information patients have consented to.
- Will be conducive to partnering with the managed care plans.
- Will need to be suitable and compliant to HIPAA Confidentiality Rules until legislation changes.
- Will accommodate a “break the glass” scenario.
- Will be patient driven, they may enter the website and execute their options.
- Will be managed by the data partner on behalf of the patient or will give the patient directions on how to manage their consent via the website.
- Or, the data partner will tell the AMIE operations team and consent would be managed by the IT team.
- Have the choice to “opt out” of allowing their medical records to be available through the exchange and in doing so sign a disclaimer that they understand that their care may not be optimal due to the restricted availability of medical records in a paper format.
- Sign a consent indicating they acknowledge the benefit of the AMIE application and agree that their records should be available through the exchange.
- The patient would understand that their choice is an “all or nothing” choice, which means they can not ask to restrict release of their records in certain settings.
- The patient would understand that they may choose to opt out at some point after authorizing their records to be available on the exchange, should a diagnosis arise that would be conducive to them doing so.

Each data partner has a consent process in place. Will they be agreeable to incorporate AMIE consent into their Notice of Privacy Practices