WISHIN

Wisconsin Statewide Health Information Network

2011

Consent Management Ad-Hoc Workgroup Deliverable

CONTENTS

AKNOWLEDGEMENTS

The completion of this document was made possible through the generous contributions of members of the WISHIN Consent Management Ad-Hoc Workgroup.

Workgroup Members
Ken Letkeman
Dave Lundal
Kim Pemble
Will Weider

SCOPE OF CONSENT MANAGEMENT AD-HOC WORKGROUP

The Technical Advisory Committee Consent Management Ad-Hoc Workgroup was formed to evaluate the technical feasibility of consent management options prepared by the Policy Advisory Committee and presented to the Technical Advisory Committee on August 22, 2011. The Policy Advisory Committee presented the following three options for consent management:

- **Option 1:** Exclude mental health providers (i.e., those subject to mental health consent laws) from participating in WISHIN's Phase II exchange.

- **Option 2:** Include mental health providers, but exclude §51.30 "treatment records" from WISHIN's Phase II exchange.

- **Option 3:** Create consent management process to allow mental health providers to participate in Phase II exchange and allow §51.30 "treatment records" to be exchanged.

During the Technical Advisory Committee on August 22, 2011, Technical Advisory Committee members determined that **Option 1** required no further evaluation since this option will limit large segments of healthcare information and will exclude providers from the WISHIN Phase II exchange. The Consent Management Ad-Hoc Workgroup was tasked with completing an evaluation of **Options 2 & 3** to present a recommendation to the WISHIN Policy & Technical Advisory Committees.

To provide a recommendation to the WISHIN Policy & Technical Advisory Committees, the Consent Management Ad-Hoc Workgroup completed the following items:

1) Contacted most commonly used EHR and HIE vendors to discuss current functionality and any future plans regarding consent management capabilities.
2) Discussed the technical feasibility of Options 2 & 3, including the estimated level of effort associated with each option.
3) Discussed the estimated costs of Options 2 & 3 for WISHIN and participants.

The subsequent sections of this document summarize the research and discussions completed by the Consent Management Ad-Hoc Workgroup.

Discussion of EHR & HIE Vendor Current Functionality

To evaluate the technical feasibility of **Options 2 & 3**, the Workgroup contacted EHR and HIE vendors to discuss current functionality and any future plans regarding consent management capabilities. To reduce the variability in responses, Workgroup members asked EHR and HIE vendors the standard set of questions contained in the table below.

#	Question
1	**How does your product segregate sensitive health information, such as mental health records, from general health information?**
2	**Do you have the ability to manage consent?** **a) If so, please describe your capability in detail.** **b) If not, is this capability included in your roadmap?**
3	**What is the complexity of customizing the product to accommodate various consent management approaches (consent at every transaction, blanket consent, etc.)?**
4	**Does the product comply with Enterprise Service Bus (ESB) standard?**

It should be noted that Gartner and Forrester do not have analyst reports available for EHR and HIE vendor capabilities. Gartner intends to cover this space in late 2011 to early 2012.

EHR Vendor Current Functionality

Workgroup members contacted representatives from the following EHR solutions: AllScripts, CattailsMD, Cerner, Epic, and MEDITECH. Information was not submitted by AllScripts and Cerner to include in this document.

#	Questions & Vendor Responses
1	**How does your product segregate sensitive health information, such as mental health records, from general health information?**
	CattailsMD §51.30 documents in CattailsMD are referred to as "Psych records." CattailsMD secures these documents based on a user security flag. Only users who are Psych providers would have this security flag and can see the §51.30 documents. CattailsMD also has a feature to create Psych "second note" that is not a §51.30 document. This gives non-Psych providers some insight into the patient, but keeps protected information confidential.
	Epic Customers can choose to mark certain patients as restricted. If a patient is marked as restricted, Care Everywhere will not respond to requests for information for that patient and no information will be sent for that patient via Care Everywhere. Customers can choose to mark certain departments in their facility as restricted. Even with the patient's authorization, summaries for visits that occurred in these restricted departments are not sent via Care Everywhere. However, all of the patient's results are sent by Care Everywhere, including lab and other results from visits in restricted departments. Similarly, all patient-level information (such as allergies, medications, problem list entries, and histories) is sent by Care Everywhere regardless of the visit in which it was documented.

#	Questions & Vendor Responses
	MEDITECH Meditech transcribed reports are assigned to client customizable document types. Many clients use this capability to create a document title for sensitive records which can be restricted in how those records are accessible by users and disclosed in any way. Additionally, Meditech clients can restrict access by departments, which is a common practice for behavioral health records. All of these restriction approaches are specific to transcribed reports. These techniques do not apply to lab results or medications, including psychiatric medications.
2	**Do you have the ability to manage consent?** **a) If so, please describe your capability in detail.** **b) If not, is this capability included in your roadmap?**
	CattailsMD CattailsMD does not have the ability to manage consent. It does have capabilities to specifically restrict PHI access from certain people (e.g. minor child from parent(s)) but there is no explicit means to track consent. CattailsMD does have a means to track Requests for Medical Records, but it is fundamentally different from managing consent. Marshfield Clinic participates in the NwHIN and securely exchanges documents with SSA using CattailsMD. To accomplish the release for these documents, Marshfield Clinic requires that the SSA send consent for the release of information and that consent information is stored in CattailsMD. The consent form, which the SSA has the patient sign, authorizes the release of medical information for a specific data range – note that the consent form that is received electronically is the exact same request form that Marshfield Clinic would receive from the state SSA office for a manually initiated release of information.
	Epic Yes - Customers can choose to manage patient authorization within Care Everywhere and have certain options to determine in what circumstances authorization is required. Authorization requirements affect whether or not a customer's system will respond to requests for information from outside organizations. If patient authorization is required, then in advance of a visit to an outside organization, the patient can authorize the organization to disclose his records using Care Everywhere to any outside organizations or to a set of specified organizations at which he might present for care. This authorization can be set to expire after an interval of the patient's choosing.
	MEDITECH Consent management is not automated within Meditech outside of some sites that scan medications for online access.
3	**What is the complexity of customizing the product to accommodate various consent management approaches (consent at every transaction, blanket consent, etc.)?**

#	Questions & Vendor Responses
	CattailsMD Marshfield Clinic is the developer of CattailsMD and as such, has the capacity to change in any way. However, this "consent" feature (consent at every transaction, blanket consent, etc.) has not been requested by a customer and as such, it has not been prioritized and there are no requirements for it at this time. In order to give an accurate estimate of the complexity and timeline, one would need some high-level scope of the problem.
	Epic See questions 1 and 2.
	MEDITECH Less complex than mastering cold fusion, but not by much.
4	**Does the product comply with Enterprise Service Bus (ESB) standard?**
	CattailsMD For the SSA project (NwHIN), Marshfield Clinic integrated the ApeniMED platform for HIE connectivity and exchange. ApeniMED does employ an ESB standard in their gateway product.
	Epic Additional information is needed to answer this question. Generally, Care Everywhere follows interoperability standards defined by organizations such as HL7 and IHE, and details on the standards currently supported can be provided if needed.
	MEDITECH Meditech itself does not support such SOA application access, but is possible that 3rd parties have or could provide such support.

HIE Vendor Current Functionality

The Workgroup contacted the following HIE vendors for information: Axolotl, Medicity, and Microsoft.

#	Questions & Vendor Responses
1	**How does your product segregate sensitive health information, such as mental health records, from general health information?**
	Axolotl If a patient elects not to share certain data, such as sensitive data related to HIV/AIDS, substance abuse, mental health, etc., or is unable to specify that the data should be shared, it will be withheld from the patient's accessible aggregated health record, and the user will not be able to reference and consider the patient data in question as part of the overall care/treatment plan.
	Medicity Medicity's platform uses HL7 confidentiality indicators to secure sensitive health information. When received, these indicators flag sensitive health information such as mental health records, and the Medicity platform can block these results from view if a user does not have the rights to view this type of information.

#	Questions & Vendor Responses
	Microsoft We attach meta data tags to incoming messages at the time of parsing, and these tags can include meta data about sensitivity of health information as long as the customer (participant) notifies us in advance of how to recognize the information (ie message tags, specific ICD codes, etc.). We can assign permissions to view data based on the meta data tags we apply at the parsing stage, enabling the overall HIE system to be configured to follow a number of different policy models. In general we recommend participating providers obtain patient consent before submitting sensitive health information to the HIE, and in the absence of that consent then participants should filter sensitive information from being sent to the HIE.
2	**Do you have the ability to manage consent?** **a) If so, please describe your capability in detail.** **b) If not, is this capability included in your roadmap?**
	Axolotl The Elysium Exchange platform provides a highly flexible and configurable patient consent module. The module supports the ability for users to: • Request "break the glass" one-time access • For patients to set consent to share data • For patients to give consent to disclose records. The consent to share data component is flexible; it can be configured to accommodate community-wide sharing, or practice/user-specific sharing. The consent to disclose records component enables patients to specify which records they want to submit to the HIE, and which they do not. Existing consent status may be imported to the Elysium consent module through standard or proprietary interfaces, based on the capability of the system providing the consent status.
	Medicity Yes. Medicity's Patient Consent framework is configurable according to an HIE's policies and supports both opt-in and opt-out patient consent models. Patient consent is a function of Medicity's Identity Management Services and a Patient Consent Management Tool is available for the HIE to use to manage the consent status for their patient population. Medicity's Patient Consent framework supports both opt-in and opt-out patient consent models, which an HIE may configure according to its policies. • For the opt-in consent model, a patient has to opt-in before their data will be available (the default status is that patient data is not available until the patient opts-in). When a patient goes to a healthcare facility to seek treatment, the system will prompt the admin clerk to ask the patient for consent before the patient's data will be available for viewing in ProAccess. Medicity's Patient Consent framework provides a variety of consent options to support the HIE's policies. For example, the patient can opt-in all or a subset of their data, give access to all treating providers or a select few, and they can specify a time limit for having their data available for viewing in the HIE. Typically the patient has to sign a consent form, then the admin clerk uses the Patient Consent Management Tool to change the patient's status to opt-in. Patient consent settings can be changed at any time should the patient choose to revoke their opt-in status at a later date. • For the opt-out consent model, a patient has to opt-out before their data is excluded (the default status is that patient data is available until the patient opts-out). If the patient choses to exclude all or a subset of their data from the HIE, the patient would complete an out-out form and an HIE administrator would use the Patient Consent Management Tool to change the patient's status to opt-out. Patient consent settings can be changed at any time should the patient choose to participate at a later date.

#	Questions & Vendor Responses
	Microsoft Yes of course. Many models can be enabled and either opt in or opt out models are possible. Consent status can be documented in existing registration systems and the consent information can be forwarded to the HIE system as a flag included in the HL7 ADT feed. Or consent status can be documented by authorized users through a configurable web based user interface.
3	**What is the complexity of customizing the product to accommodate various consent management approaches (consent at every transaction, blanket consent, etc.)?**
	Axolotl The way the system behaves based on known consent conditions is configurable. For example, is patients opt in, they may be opting in to share with the entire community, or they may have to specify practices and entities to share data with. The consent modules flexibility is also highlighted by the ability to configure the system to react differently based on unknown consent conditions. For example, if a patients consent is unknown, the system may automatically treat the consent as: • "Opt-in" to automatically share with the community • "Opt-out" to deny community access • "Emergency only" to allow community access if an emergency situation is declared
	Medicity Medicity's Patient Consent model provides a variety of granular consent options. Patient consent can be specified as a "blanket" consent for all providers, or specified at a specific provider-level. It can also be specified for a specified time period and can be set differently for sensitive health information. For example, a patient could opt in all of their general health information, but opt out their sensitive health information, or could opt in all of their data for just 1 year. Medicity's platform does not currently offer patient consent to be defined at the individual encounter level, but if a patient wants a specific encounter to not be available in the HIE, this encounter could be flagged as containing sensitive health information and could be opted out.
	Microsoft Consent can be "blanket" or at the encounter level. Linking consent information to the encounterID is necessary to accommodate scenarios where patients change their mind about consent from one encounter to another and to maintain history of these changes.
4	**Does the product comply with Enterprise Service Bus (ESB) standard?**
	Axolotl Yes. The platform offers a rich, ESB standards-based set of web services for application integration. The integrated applications, either custom developed or provided by third-party vendors, can interoperate seamlessly with Elysium applications, such as the EMR, VHR, patient index and clinical summary. The web services offered by Open Access are highly secure and designed to support high transaction loads. The web services are built using Java EE. They use an enterprise service bus for event-driven communication, and uses SAML and WS-Security for authentication and authorization.
	Medicity Yes. In addition, Medicity also interoperates with most other standards and de facto standards for interoperability such as: • Services: SOAP, Web Services, HTTP-Rest, SMTP, MLLP, etc. • Content: HL7 v2.x, HL7 v3 CDA, CCD/CCR/C32/C37, XML, XDM, XDS-MS, etc. • Gateways: IHE XCPA, XCA, NwHIN Patient Discovery, Query for Documents, Retrieve Documents, etc. • Security: WSS, SAML, ATNA, CMS, S/MIME, VPN, TLS, etc.

#	Questions & Vendor Responses
	Microsoft Not sure what this means. If it means consent information can be passed using a standard web service, the answer is yes.

Discussion of Technical Feasibility

EHR and HIE vendor research indicates that **Option 2** is technically feasible. The majority of vendors have the capability to flag sensitive health information to be excluded from the exchange. **Option 2** closely resembles the current practices Wisconsin organizations are using in the Wisconsin Health Information Exchange (WHIE) and Epic Care Everywhere. An item that requires further discussion however, is that even though consent is being obtained at every encounter for participants in the Epic Care Everywhere exchange, Care Everywhere excludes the exchange of §51.30 treatment records.

Based on EHR and HIE vendor research, it is unclear if **Option 3** is technically feasible. The Workgroup did not identify a commercially available technical solution for the implementation of **Option 3**. Although unclear, the implementation strategy used by the Nebraska Health Information Initiative (NeHII) suggests that **Option 3** may be technically infeasible. NeHII is implementing a separate exchange for mental health, electronic Behavioral Health Information Network (eBHIN), which is expected to go live in late summer 2011.

Discussion of Estimated Costs

Option 2 is estimated to be less costly than **Option 3** for WISHIN and WISHIN participants. **Option 2** is technically feasible using commercially available technical solutions and closely resembles current practice for the exchange of health information. This implies that organizations participating in WISHIN will need to implement fewer operational changes.

Since it is unclear if there is a technically feasible solution for **Option 3**, the Workgroup could not discuss estimated costs.

Consent Management Ad-Hoc Workgroup Recommendation

The Consent Management Ad-Hoc Workgroup recommends that WISHIN plan to implement **Option 2** in their Phase II operations based on current Wisconsin mental health laws. Research compiled by the Workgroup suggests **Option 2** is:

- Technically feasible,
- Implemented by other well-established HIEs, and
- Less onerous for WISHIN participants due to fewer operational changes.