Fragen zu „Standards und Architektur „eHealth Schweiz“

Name der Organisation:	Interessengemeinschaft eHealth
Name und Funktion der Ansprechperson:	Urs Stromer, Präsident
Adresse und Mail:	stromer@ig-ehealth.ch
Ort und Datum:	Bern, 19. Dezemeber 2008

Besten Dank für die Rücksendung an stefan.wyss@ehealth.admin.ch bis zum **19. Dezember 2008**.

	Zustimmung	Zustimmung mit Vorbehalten	Ablehnung
1. Grundsätzlich Die ersten Vorschläge zu „Standards und Architektur“ entsprechen unseren Vorstellungen und sind für das Thema zielführend.	☐	☒	☐
Begründung Vorbehalt/Ablehnung: **Die Vorgehensweise nach IHE als Basis für eine schrittweise, benutzeranforderungs-gesteuerte Spezifikation von Anwendungsfällen, basierend auf geltenden internationalen Industriestandards, erachten wir als sinnvoll und zielgerichtet.**			
2. Vorschlag 1: Grundsätze als Basis (Seite 2) Die allgemeinen Grundsätze, die als Basis für die Vorschläge zu Standards und Architektur dienen, entsprechen unseren Vorstellungen.	☐	☒	☐
Begründung Vorbehalt/Ablehnung: Vorbehalt: Datenschutz und Datensicherheit, Zweckbindung, informationelle Selbstbestimmung, Haftung und Aufsichtspflichten: Die Datenschutz-, Zweckbindungs-, Selbstbestimmungs- und Policy-Vorgaben sind durch überprüfbare, kantonsübergreifend harmonisierte Rahmenbedinungen festzulegen. Die Überprüfung der Einhaltung dieser Vorgaben ist Sache einer durch Bund und Kantone zu beauftragenden resp. legitimierenden, unabhängigen Überwachungsstelle (analog der Selbstregulierungsorganisationen bei der Geldwäscherei oder den Revisionsgesellschaften zur Überwachung der rechtmässigen Buchführung in Gesellschaften). Dezentrale Strukturen: Diese sind nur bedingt sinnvoll da sich die Systemkomplexität, insbesondere in der Datenzugriffsauthorisierung explosionsartig erhöht und verteuert. Es ist anzustreben, ein nationales Policy und Rollenkonzept mit national gültigen Zugriffsvarianten zu verankern (gemeinsames Regelwerk basierend auf gemeinsamen Metadaten und Attributen).			

Index der Behandelnden: Authorisierungen für Datenzugriffe müssen auf einem zentralen Regelwerk aufsetzen. Da die Zugriffrechte primär von den Rollen und den Identitäten der Behandelnden abhängen, wird eine dezentrale Haltung der Informationen zu den Behandlenden und den dazugehörigen Rollen und Rechten sehr komplex. Es wäre im Sinne der Reduktion der Komplexität des Systems, alle Behandelnden in einem zentralen Verzeichnis zu führen. Die Mutationen werden jedoch vor Ort von den verschiedenen Organisationen vorgenommen, also dezentral verwaltet.

Die Protokollierung der Zugriffe, insbesondere der Notzugriffe, ist als Komponente zu erwähnen.

Völlig offen gelassen wird der Umgang mit Systemen, Infrastrukturen und Komponenten aus dem angrenzenden Ausland. Der Entscheid, sich internationalen Standards anzuschliessen, ist eine gute Basis. Hinweise zur Erreichung interoperabler Prozesse mit dem angrenzenden Ausland wären sicher hilfreich. Hierbei ist auch eine Priorisierung anzugeben, welche Themen angegangen werden sollen.

Hinweisen möchten wir auf die Wichtigkeit der Governance, insbesondere im Hinblich auf verbindliche Prozesse.

3. Vorschlag 2: Basiskomponenten der Architektur (Seite 4) Mit den vorgeschlagenen Basiskomponenten sind die allgemeinen Grundsätze umsetzbar.	☐	☒	☐

Begründung Vorbehalt/Ablehnung:

Vorbehalt:
Patientenindex: Die Patienten Indizes sind übergeordnet zu kaskadieren, so dass eine überregionale Patientenerkennung möglich ist.

Berechtigungssystem: Die Zugriffsrechte müssten schweizweit nach den gleichen Methoden und basierend auf gleichgelagerten Metadaten aufgesetzt werden. Die eigentlichen Regeln können sich im lokalen Kontext unterscheiden, müssen aber in ein einziges, nationales Schema passen. Hier ist auch die enge Verflechtung mit den Attributen des Behandelnden-Verzeichnisses zu beachten.

4. Vorschlag 3: Instrumente (Seite 4) Die vorgeschlagenen Instrumente, welche im Rahmen der Einführung der Versichertenkarte vorgesehen sind, unterstützen nach unseren Vorstellungen die Umsetzung der Architekturelemente.	☐	☒	☐

Begründung Vorbehalt/Ablehnung:

Vorbehalt:
Die Spezifikation der Versichertenkarte beschreibt weder Schlüsselmaterial noch die CF-Codes der Datenstrukturen (keine Definition der Anforderung wie und welche Datenbereiche geschützt werden müssen). Den Herausgebern der Karte werden keinerlei Vorgaben gemacht, wie und wo allfälliges Schlüsselmaterial oder Zertifikate auf die Karte aufzubringen sind. Die Karte genügt unserer Ansicht nicht dem verlangten Sicherheitsniveau.
Desweiteren ist die spezifizierte Versichertenkarte als Identifikationsmittel absolut ungeeignet. Für den Behandelnden ist eine einfache Identifikation des Patienten (Übereinstimmung Karte zu Patient) nicht möglich. Alle Alternativen zu einem Bild für die Identifikation (z.B. zwingende PIN Eingabe des Patienten, Unterschrift des Patienten, andere Biometrische Merkmale) sind weniger praktikabel und aufwändiger zu prüfen. Ohne Bild oder ein anderes, einfach prüfbares Identifikationsmerkmal auf der Karte, wäre der alleinige Besitz der Versichertenkarte genügend, um einen Datenzugriff vorzunehmen. Dies würde wohl gegen die vorgängig definierten Datenschutz-Grundsätze und den hohen Aufwand einer Zugriffregelung verstossen.

Berechtigungssystem: Die Zugriffsrechte müssten schweizweit nach den gleichen Methoden und basierend auf gleichgelagerten Metadaten aufgesetzt werden. Die eigentlichen Regeln können sich im lokalen Kontext unterscheiden, müssen aber in ein einizges, nationales Schema passen. Hier ist auch die enge Verflechtung mit den Attributen des Behandelnden-Verzeichnisses zu beachten.

Völlig offen und unbehandelt ist die Interoperapilität mit angrenzenden ausländischen Systemen.

5. Vorschlag 4: Prioritäre Hauptprozesse (Seite 5) Ein schrittweises Vorgehen auf dem Weg zur Interoperabilität ist richtig, und die beiden vorgeschlagenen Hauptprozesse sind aufgrund ihrer Relevanz und Häufigkeit als prioritär zu betrachten.	☐	☒	☐

Begründung Vorbehalt/Ablehnung:

Vorbehalt:
Die gewählte Strukturierung der Hauptprozesse ist zu verfeinern. Es gibt asynchrone Kommunikation (ein Dokument wird in der Infrastruktur vorgehalten, der Abfragezeitpunkt ist nicht bekannt) und synchrone Kommunikation (die Information wird umgehend verarbeitet, allenfalls wird eine Antwort ausgelöst). Die gezeigte Systemarchitektur scheint nur die asynchrone, für die Dossierbildung sicher auch relevante Kommunikation zu beschreiben. Zur Prozessunterstützung ist aber auch die synchrone Kommunikation in der Architektur vorzusehen.

Weiter empfehlen wir das XCA Profil (Kommunikation zwischen Affinity Domains) zu ergänzen sowie in eine Empfehlung der Variante XDS.a oder XDS.b auszuarbeiten.

6. Vorschlag 5: Empfohlene Standards in der Startphase (Seite 6) Die vorgeschlagenen internationalen Standards sind geeignet, die Umsetzung der Architektur und prioritären Prozesse zu ermöglichen.	☐	☒	☐

Begründung Vorbehalt/Ablehnung:

Als eine der wichtigsten Voraussetzungen erachten wir die Definition das Basisregelwerks.

Überwachung und Zertifizierung: Grundsätzlich gehen wir davon aus, dass keine Zertifizierungen notwendig sind, da diese durch die gewählte Vorgehensweise nach IHE bereits sichergestelt ist. Hierbei

würden die Beschaffenden die Erfüllung verschiedener IHE Profile in deren Ausschreibungen verlangen. Ebenfalls gehen wir davon aus, dass sicherheitsrelevante Komponenten auf internationalen Sicherheitsstandards und Zertifizierungen abstützen, z.B. EAL, BSI oder ZertES Zertifizierungen. Beim Einsatz solcher Komponenten und Produkte müsste der Nachweis durch Vorweisen der Atteste erbracht werden.

Für die Umsetzung des XDS Profils sind verschiedene weitere Profile notwendig wie CT (Consistent Time) und ATNA (Audit Trail and Node Authentication). Eine grosse Lücke besteht zur Zeit im Bereich des Authoriserungs-Managements. Es sind verschieden Bestrebungen innerhalb der IHE Community vorhanden basierend auf den OASIS Standards (XACML, SAML) Datenzugriffe zu regeln. Diese Lücke ist zu erwähnen. Es wäre wünschenswert, wenn auch aufgezeigt würde, wie diese Lücke geschlossen werden kann.