Interoperability for Mobile applications: New IHE profiles

Charles Parisot
Member, IHE International Board
Chair, IHE European Affairs Committee
Manager Standards and Testing, GE Healthcare
Deployment of the current Mobile App ecosystem in health

Successes in the Deployment of mHealth:

• Adding mobile terminals for health professionals to operate/interact with a specific Healthcare IT system or device within a care delivery organization

• Enabling patient access to a portal specific to a care delivery organization (appointments, reminders, access to results and records).

• Mobile Health management applications either stand-alone or connected each to a specific cloud-based application

➤ Mobility of access is significant
➤ But health data remains in silos
Deployment of the current Mobile App ecosystem in health

Interoperability challenges in the Deployment of mHealth

- Mobile App for health professionals
- Patient access App to a portal (appointments, reminders, access to results and records).
- Personal health management app either stand-alone or connected

Specific Healthcare IT system or device within a care delivery organization: EMR, PACS/RIS, etc.

Portal of a specific Healthcare delivery organization: hospital, insurance, laboratory, etc.

Device specific cloud-based personal health management application

Mobility increases number of silos
Access to health services: mHealth needs eHealth

The consumer challenge: Proliferation of Apps
mHealth needs eHealth interoperability to enable “portable” generic Apps

Replaces the proprietary interfaces of the Apps with a standardized interface
Access to health services: mHealth needs eHealth

* eHealth interoperability to provide an integrated and ubiquitous patient health view
mHealth needs eHealth interoperability to provide an integrated and ubiquitous patient health view.

mHealth most effective as “edge” information access/source.

Access to health services: mHealth needs eHealth
Access to health services: mHealth needs eHealth

IHE Profiles available and widely accepted for eHealth interoperability

New IHE Profiles being developed for mHealth interoperability
New profiles for IT Infrastructure

- Profile in Mobile/REST have been developed:
  - PDQm → Patient Id Mgt
  - IUA → Authentication
  - MHD → Mobile Health Document Sharing
    nicknamed “XDS on FHIR”

- REST strategy: a progressive extension:
  - HL7 FHIR is a DTSU (DSTU2 under review)
  - HL7 FHIR expected to be a standards early 2017
  - Add to existing (e.g. XDS & MHD)
  - Avoid content disruption; MHD + CDA content
IHE - MHD
Mobile device access to Health Documents
IHE - MHD Profile:

- As simple as possible on the client side, yet supports as much of XDS Document Source and Document Consumer functionality.
- Document content neutral (IHE Content profiles, CDA, DICOM, Text, HTML, etc.)
- MHD focused on supporting as small of a footprint on the client side (representational case of the client is a mobile device such as smartphone or tablet).
- Not intended to replace XDS, but augment it (edge mobile access)

Accesses: Shared Document Metadata and Documents
Technology: XML & JSON
IHE – MHD Use Cases
Mobile device access to Health Documents

- Kiosk used by patient in hospital registration departments. Likely workflow is having registration clerk ultimately pushes the button.
- PHR publishing into a staging area for an EMR or HIE/EHR
- Medical devices targeted by IHE Patient Care Devices (PCD) domain or Continua organization, submitting data and documents
- Patient or provider application that is configured to securely connect to PHR in order to submit records
- Medical Device in a referral clinic
- A general practitioner with minimal IT
Authorization services will not be centralized, national, or unified.

Authorization services will be not be healthcare provider selected.
- A patient will have their preferred authorization server,
- A healthcare provider will have to be able to support multiple authorization servers, and these servers will not be under the control of the healthcare provider.

The selection of authorization services will be a matter for negotiation among patient, authorization services, and healthcare providers.

Healthcare services will need to adapt commonly used authorization services

RESTful services will require authorization

Other options may evolve. (This is why this should be an option rather than part of the base profile.)
Choice of OAuth 2.0

- OAuth 2.0 is the dominant available framework

  - OAuth 1.x has been successfully deployed for commercial uses with web browsers.
  - OAuth 2.0 is a subsequent authorization framework that is designed to be profiled for specific uses, and to fix problems found with OAuth 1.x
Use Case with OAuth 2.0

OAuth specifically avoids specifying other traffic and coordination traffic so that different authorization methods can be employed. For example, some authorization servers use tokens and others use password traffic as part of the request process.
Future profiles for IT Infrastructure

- **Profile for Mobile/FHIR:**
  - PIXm ➔ Patient Cross-referencing Mgt
  - ACMm ➔ Alarm Communication
Providers and Vendors
Working Together to Deliver
Interoperable Health Information Systems
in the Enterprise
and Across Care Settings

http://www.ihe.net