HealthManagement
Promoting Management and Leadership

Volume 7 - Issue 5, 2007 - Country Focus:Radiology in Finland

Finnish National EHR Project: An Interoperable Infrastructure for eHealth

Author

Pekka Ruotsalainen

National Research and

Development Centre for

Welfare and Health

Stakes Unit for eHealth

and eWelfare

Helsinki, Finland

pekka.ruotsalainen@stakes.fi

The national communication platform is financed both by the Ministry of Social Affairs and Health and public and private service providers. The platform will start its service in Spring 2008 and should be fully operational by the end of 2011. The platform offers both promises and challenges. Using the national eArchive it is possible to create one virtual lifelong personal health record for every citizen which can be used for profiling, prevention and prediction of the future health status and risks.

Typical eHealth services available via the internet are booking and information services, disease and lifestyle management and home care. The eArchive also offers citizens access to his or her own EHR and audit logs generated by the eArchive. Because all official eHealth services will use the national web service platform, it is also a natural platform for future consumer-oriented eHealth services.

Background – Digitisation in Finland

The first eHealth strategy established by the Ministry of Social Affairs and Health was published in May 1996 built around the principle of secure information sharing and ICT support for seamless citizen-centred care. This strategy was updated in 1998 with the following targets: adoption of EHRs in all levels of care, nationwide interoperability, high-level security and privacy protection and citizens' access to their records via the internet. This strategy was realised by the implementation of regional cooperative EHR systems (RHIS) with common middleware services. RHIS supported the transmission of eReferrals, eConsultation messages and digitalised images.

Structure of the Finnish EHR

In Finland every health organisation has the responsibility to manage and archive health records. Inside the service organisation the health record is personal and lifelong. Based on national regulations health records must be archived up to 100 years and images should be archived for 20 years.

In Finland the collection of care information is based on documents. Those documents represent snap-shots of the dynamic care process. For security and confidentiality, after every care episode, the responsible physician must sign the EHR. The internal organisation of the Finnish health record is very close to the structure defined in the open EHR standard. The EHR has folders for every specialty and inside a folder there is a set of cumulative episodes. Episodes are organised under headings. Each headed section is lifelong and cumulative.

Securing the Future of Healthcare

In 2001, the Finnish government launched the national programme for securing the future of healthcare. One of the eighteen projects of the programme concerns the implementation of national, interoperable EHRs. Messaging methods are based on HL7 CDA and DICOM messages for communication. A national core data set was created for semantic interoperability.

The long term tradition in Finland has been to develop both strategy and supporting legislation in parallel. A new act regulating the management

and use of electronic health information has been developed. This act regulates the collection and disclosure of EHRs and sets minimum security and privacy protection rules. The updated eHealth strategy and new legislation form the road-map for the implementation of future eHealth services in Finland.

The national communication architecture is targeted to support both the technical and semantic interoperability of EHRs and to solve the problem of the longterm availability and usability of EHRs. Security services are also one of the key functions of the platform. In the architecture, the web-service platform acts as an integration machine. Information between legacy systems and common services are transferred in the form of documents. Citizens and patient are connected to the eArchive via web services.

Technical interoperability is achieved using standardised messages. Messages accepted at the present time are HL7CDA R2 and DICOM. ePrescriptions are transferred in the form of HL7 v.3 messages. All messages have a header with harmonised meta-data and a structured body section supporting the previously- mentioned EHR structure.

Semantic interoperability is archived by making the use of national core data sets, selected classifications and EHR headings mandatory. All terms and classifications can be downloaded from the term code server. Long-term availability of records is achieved by the development of a centralised EHR archive. For security, all documents are signed electronically and transferred in a Simple Object Access Protocol (SOAP) envelope. Healthcare persons and entities are identified and authorised using the common PKI-service. All health professionals have a health professional smart card.

Common Services

Key common services are registration of EHRs, eArchive, consent management, certification service and code and term service. The registering service is the key tool to locate and manage EHRs.

The role of the eArchive is to preserve, disclose and destroy records. The disclosure of EHRs is based on policy rules. In Finland, preconditions for any EHR disclosure are the presence of doctor-patient relationship, patient’s consent or explicit legislation. It is the responsibility of legacy systems to create the relationship credential and consent document. A policy engine has been included to the SOA service layer to control the disclosure of EHRs. The eArchive has to prove the availability and security of records during preservation.

The main task of the eArchive is to preserve narrative EHRs, pictures, images and bio-signals. Existing PACS/RIS systems send pictures selected for long term preservation or disclosure in DICOM document format to the eArchive. The national consent service stores all consent documents. Patients maintain the right to check and change their active consent profile. The eArchive must check consent before any data disclosure. National certification services are intended both for healthcare entities and health persons. There is also a national certification service for citizens.

Requirements for the Users of National Services

The main users of common services are legacy systems and patients. Present legacy systems are not ready to be connected to common services. They should be updated and new services should also be developed for citizens. All computer systems connected to the national platform should be certified against functionality, interoperability and security.

Legacy systems should implement the following new services before the use of national services:

1. A data entering application to support common headings, terms, classifications and the core data set;
2. Creation of consent document and relationship credentials;
3. Capturing data from the local database;
4. Creation of HL7CDA and DICOM messages;
5. Creation, preservation and access requests which are sent to the eArchive;
6. Viewing received EHR-messages; and,
7. Generating audit logs.

A secure web service will be developed for citizens accessing the eArchive via the inter-net. A smart citizen card and certification services should be used for security.

Published on : Sat, 15 Dec 2007