*Medical Infobahn for Europe*
*A. Hasman et al. (Eds.)*
*IOS Press, 2000*

# Role-Based Access to Patients Clinical Data: The InterCare Approach in the Region of Crete

G. Potamias[1,2], M. Tsiknakis[1], D. Katehakis[1], E. Karabela[1], V. Moustakis[1,3] and S. Orphanoudakis[1,2]

[1]*Center of Medical Informatics and Health Telematics Applications (CMI-HTA), Institute of Computer Science (ICS), Foundation for Research and Technology – Hellas (FORTH), P.O. Box 1385, GR 711 10, Heraklion, Crete, Greece, Tel: +30 (81) 391693, fax: +30 (81) 391601, E-mail: {potamias, tsiknaki, katehaki, karabela, moustaki, orphanou}@ics.forth.gr, URL: http://www.ics.forth.gr*

[2]*Department of Computer Science, University of Crete, P.O. Box 2208, GR 714 09, Heraklion, Crete, Greece*

[3]*Dept. of Production Engineering and Management, Technical University of Crete, GR-731 00, Chania, Greece, moustaki@logistics.tuc.gr*

**Abstract.** The basics of a particular Integrated Electronic Health Record (I-EHR) implementation are presented, as realised by the Patient Clinical Data Directory (PCDD) system. PCDD operates within the context of HYGEIAnet, the Integrated Healthcare Telematics Network of Crete. PCDD is based on a federation of autonomous information systems and provides to its authorized users alternative views of the health record as well as access and retrieval services to its geographically distributed segments. The data model of the PCDD is based on the Subjective Objective Assessment Plan (SOAP) model that originates from the primary healthcare domain. Access to detailed information on particular patients healthcare encounters is delivered via role-based authorisarion privilages and controls. The administration of the national healthcare organizations' business rules, for different user-groups, is made via a specially tailored and developed rule-editor.

## 1. Introduction

During a single healthcare episode many professionals, involved in a variety of medical acts, administer medical care. Healthcare administration personnel, healthcare professionals, social care professionals, as well as patients need to selectively interact with health-related information. Each user group has different needs in terms of information access, security, and quality of service, and is involved in different medical acts and healthcare procedures.

The main middleware enabling services supporting the creation of an *Integrated Electronic Health Record* (I-EHR) from its distributed segments are among others:

- a set of *security services* which provide safe access to the confidential clinical information and record any interaction with the I-EHR,
- the *information systems registry* which includes information about the clinical information systems that belong to the federation,
- the *patient registry* which locates the patients of the regional network, and
- the *medical encounter registry* which includes patients' encounter information, and facilitates the access to the related clinical information.

In this paper an approach to I-EHR services is presented, as designed, developed and deployed in the context of the HYGEIAnet integrated health telematics network in the region of Crete [1]. In particular, I-EHR services are offered via a *Patient Clinical Data*

*Directory* server which, among other, offers *role-based authorisation access* to distributed and heterogeneous segments of patients clinical information. Next section presents the basics (architecture, background technology, functions and operations) of PCDD. In section 3 the principles, the specification, and the realization (via a specially tailored and developed rule-editor) of role-based access control are presented. The last section concludes the presentation and points to some future development plans.

## 2. Patient Clinical Data Directory: Services, Components and Data Models

The main objective of the *Patient Clinical Data Directory* (PCDD) middleware is to provide basic support for I-EHR services in a consistent, reusable, and extensible way. PCDD indexes patient and feeder system identification, as well as information about the clinical objects of patients' EHR segments. This information is accessible to *authorized* users through stable IDL interfaces.

Figure 1 shows the architecture of the PCDD. In the core of the PCDD middleware lays the X.500/ LDAP directory. The PCDD server is a CORBA server that exports a number of public and stable IDL interfaces to be used by other middleware and user-oriented services. The PCDD server communicates with the directory using the LDAP protocol.

*Data Models:* Information about clinical objects in the directory refers to clinical patients' data that are produced during the communication about the patient, between two or more individuals, at least one of whom is a member of the healthcare team currently involved. This communication is called *encounter*. The most common type of an encounter is a visit to a medical office, clinic, or primary healthcare center. Medical encounter entries in the directory follow the *Subjective Objective Assessment Plan* (SOAP) model that is an approach for recording clinical data generated during the contact of a patient with a healthcare provider [2] (see Figure 2). *Subjective* refers to the reason of the contact (i.e. the context of the encounter). *Objective* applies to medical examinations requested or reviewed during the contact e.g. blood examination, etc. *Assessment* refers to the clinical diagnosis and associated reports. *Plan* refers to the clinical actions that must be taken, i.e. the treatment plan (drugs, surgery, etc.).

*Clinical Feeder Systems:* PCDD provides the information required for accessing clinical multimedia information directly from its source, i.e., PCDD feeder systems. *Feeder systems* may support a wide variety of access methods ranging from human-mediated, to CORBA object references, and HTTP URLs. In general, feeder systems update the directory in a bulk-load fashion. Each feeder system is associated with a dedicated gateway that facilitates data extraction from the feeder system. Gateways get data from the feeder system, map them to the model of the directory, and translate them into LDAP statements, which are stored in a standard LDAP *modify* file. Since feeder systems are in general heterogeneous, thes gateways may take different forms. Possibilities include but are not limited to ODBC/ LDAP, and DICOM/ LDAP gateways. PCDD does not deal with the semantic mapping problem directly. It is the responsibility of a feeder system to map an export schema of its information model to the directory information model. The underlying assumption is that a human who understands the semantics of both the directory model and the export schema of the feeder system provides this mapping system [3], [4]. A minimal export schema of a feeder system should express the existence of a patient's EHR segment by providing patient identification attributes.

In its current deployment status (as for January 2000), PCDD offers access to various distributed healthcare sites (medical units) in the region of Crete, and to respective distributed clinical information systems (the legacy feeder systems).

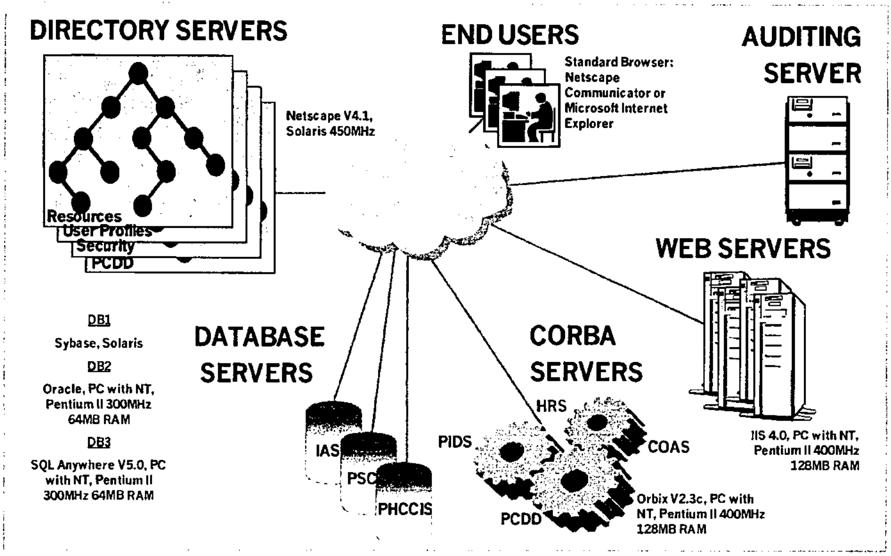

DIRECTORY SERVERS
Resources
User Profiles
Security
PCDD
Netscape V4.1, Solaris 450MHz
END USERS
Standard Browser: Netscape Communicator or Microsoft Internet Explorer
AUDITING SERVER
WEB SERVERS
IIS 4.0, PC with NT, Pentium II 400MHz 128MB RAM
DB1
Sybase, Solaris
DB2
Oracle, PC with NT, Pentium II 300MHz 64MB RAM
DB3
SQL Anywhere V5.0, PC with NT, Pentium II 300MHz 64MB RAM
DATABASE SERVERS
IAS
PSC
PHCCIS
CORBA SERVERS
HRS
PIDS
COAS
PCDD
Orbix V2.3c, PC with NT, Pentium II 400MHz 128MB RAM

*Figure 1. PCDD Related Applications, Services and Components.*

In particular, PCDD accumulates, indexes, stores and provides the means for accesing patients' clinical information from the *Primary Health Care Center Clinical Information System* (PHCCIS- located in more than 9 isolated HCCs in the Crete region), and from the *Pre-Hospital Emergency Management System* (PHEMS- installed in the central *Emergency Co-Ordination Center* of Crete, located at Heraklion).

*Encounter-based view of patients clinical encounters:* The objective of the PCDD service is to deliver an *encounter-centered* view of the patient's I-EHR. It utilizes the *PCDD Update* interface to provide a consistent way to locate, and access information about a patient's EHR segments. PCDD indices both structured and unstructured information that is provided by co-operating information systems, without imposing any constraint on their internal operation or their interface, beyond the medical encounter level. Since electronic records can provide much easier navigational facilities, navigational issues will become even more important in the future, mainly because of the end-user requirements to have similar interfaces in terms of look and feel. In addition any such interface should be able to work in a secure environment.

Guided by the aformentioned specifications, an advanced and fully operational Graphical User Interface (GUI) has been developed. The GUI encompasses operations for: easy parameterised (by date, clinical information system, place, time etc) *search* and respective *query formulation*, *regional statistics*, *snapshots* of patient's medical encounters and *messaging* (exchanging patient's clinical snapshots between co-operating physicians etc).

| | | Subjective | Objective | | | | | Assessment | Plan |
|---|---|---|---|---|---|---|---|---|---|
| Date | Doctor | Reason | Clinical Exam | Gynecological Exam | Blood Exam | Biochemical Exam | Imaging Exam | Diagnosis | Action |

*Figure 2. Medical Encounter Entries in the Directory Follow the SOAP Model*

## 3. Role-based Access to Patients' Clinical Data

Several levels of security exist; namely information system security, operating system security, database system security, network security, communication security, etc. The presented approach does not face security isolated in a per-process (or use-case) point of view. Instead it follows a two level approach that can guarantee greater availability, *integrity*, and *confidentiality*. The first level of security is implemented by means of the HYGEIAnet Virtual Private Network (VPN) that offers Committed Information Rate (CIR) for medical applications and is suitable for both auditing and statistics. This security level increases service availability and can implement restrictions on virtual servers and directories. The second security level can guarantee secure communications through insecure channels by means of encrypted and authenticated communications, and can be applied not only inside firewalls but also to every computer. This way it can guarantee secure connections for both remote users and among sites.

For the PCDD to be able to offer secure services it needs to be able (a) to *authenticate* each client's principal identity, role and sensitivity, and (b) to transmit information *confidentially* and with integrity. It is evident that the existence of a trust infrastructure needs to evolve as part of the underlying regional information infrastructure [5]. This way security and confidentiality services can be based on a regional certification authority, which will provide digital certificates to healthcare facilities and human resources.

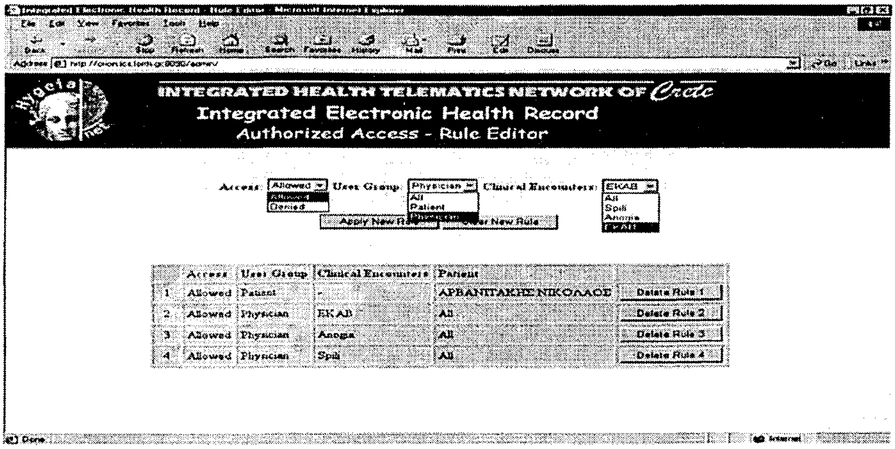
The purpose of the certification authority is to certify *the role* and *authority* of both users, and services (or applications) within the regional healthcare network. The combination of digital signatures for authentication, public key cryptography for recipient authentication, and Secure Socket Layer (SSL) protocols for secure data-transfer, provide the necessary technological framework for secure communication of healthcare related information across the Internet.

*Access Control:* Access control is achieved by means of *user profile* information (PCDD server communicates with a *Healthcare Resource Directory - HRD*, via a dedicated CORBA-based IDL interface). In this context, any patient should be able to have complete access to all personal information. A physician should have access to all information that has been provided by him, as well as to his/ her referral data. In addition patients should be able to grant and restrict access to their personal information.

In emergency healthcare episodes, the defined *actors* (user groups and roles) should have the right to access any patient's medical record. These emergency accesses should, however, be logged. More emphasis needs to be paid on auditing "*who* accesses *what* type of information at *what* time," instead of trying to enforce very tight security constraints.

### *3.1 Administrating Access Control: The Rule Editor*

The way medical record should be managed within a healthcare delivery organisation is formulated in an *access control policy*. This policy has its origin in legislation and includes all aspects of access control and security. Many of those aspects have an impact on the functioning of the information system, which handles medical record information. Those aspects of the access control policy, which have an impact on the information system, are described as *access control rules*. Based on these principles and guidelines, a *Rule-Editor* module has been designed and developed within the LDAP context; so, sharing structures and objects with the PCDD server. The rule editor is for use by the PCDD *administrator*.


INTEGRATED HEALTH TELEMATICS NETWORK OF Crete
Integrated Electronic Health Record
Authorized Access - Rule Editor
Apply New Rule
Clear New Rule
Done
Internet

Access: Allowed (Allowed, Denied) User Group: Physician (All, Patient, Physician) Clinical Encounters: EKAB (All, Spili, Anogia, EKAB)

| | Access | User Group | Clinical Encounters | Patient | |
|---|---|---|---|---|---|
| 1 | Allowed | Patient | - | ΑΡΒΑΝΙΤΑΚΗΣ ΝΙΚΟΛΑΟΣ | Delete Rule 1 |
| 2 | Allowed | Physician | EKAB | All | Delete Rule 2 |
| 3 | Allowed | Physician | Anogia | All | Delete Rule 3 |
| 4 | Allowed | Physician | Spili | All | Delete Rule 4 |

*Figure 3. Administrating Access-Control via a Rule Editor.*

The administrator may *add/ apply* and *delete* rules according to: (i) the national healthcare legislation (for keeping and sharing clinical data), and (ii) the specific healthcare (public or private) organisation's security and authorisation policies. Access control operates on patients' medical encounters *allowing/ denying* access to specific segments of patients' clinical information. The format of each rule is kept as simple as possible. So, the basic operators of an access rule are: (a) the *Access* {Allowed, Denied} operator, (b) the *User_Group* {Physician, Patient/ Citizen} operator, and (c) the *Clinical_Encounter* operator. It should be emphasized that the whole control strategy is implemented within the LDAP framework. The rule-editor component is an application, implemented by means of Perl CGI scripts, and operates over a normal Web browser (see Figure 3).

## 4. Conclusions and Future Work

Sharing of information resources is generally accepted as the key to substantial improvements in productivity and better quality of service. In this environment, diverse user groups require secure customisable access and sharing of information residing at geographically distributed autonomous information systems. In this paper the Patient Clinical Data Directory service was presented, as the core component for an implementation of the I-EHR. PCDD integrates heterogeneous patients' medical encounters from distributed clinical information systems that operate in respective healthcare units on the Crete island.

A key-feature that enhances PCDD operations, making it more reliable for the healthcare community, is a specially tailored and developed rule-editor for administrating the access to medical data, based on pre-specified security policies, users' roles, and privilages. In its current version, access control is put on the encounter-level of patients' history. It is in our future plans to put the control over the *data-level* by letting healthcare actors to view parts of the medical encounter (e.g., values of lab tests). Towards this goal we plan to integrate (via customised IDL interfaces) PCDD with the *Information Access Control Server* (IACS), as specified and developed in the context of the InterCare project (HC 4011) [6].

**Acknowledgement.** This work is partially supported by the InterCare (European Healthcare Telematics Application Programme, HC 4011) project.

## References

[1] M.Tsiknakis, C. Chronaki, S. Kapidakis, C. Nikolaou and S. Orphanoudakis, An Integrated Architecture for the Provision of Health Telematic Services Based on Digital Library Technologies, *International Journal on Digital Libraries*, Vol. 1, No. 3, 1997, pp. 257-277.

[2] M. Bainbridge, P. Salmon, A. Rappaport, G. Hayes, J. Williams and S. Teasdale, The Problem Oriented Medical Record - just a little more structure to help the world go round?, *Proceedings of the 1996 Annual Conference of PHCSG*, Downing College, Cambridge, UK, September 1996

[3] W. Grimson and D. Berry, Synapse Federated Healthcare Record Server: Software Requirements Specification of the Federated Healthcare Record Server, HC 1046, *Synapses Deliverable User 1.1.1* (Part B), Dublin Institute of Technology, 1997.

[4] InterCare Consortium, InterCare Common Product Interface Specifications - Functional and Architectural Environment of InterCare Electronic Patient Dossier Server (IC-EPDS), HC 4011, *InterCare Deliverable D3.2*, pp. 9-35, 1999.

[5] Y.-H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick and M. Strauss, REFEREE: Trust Management for Web Applications". In *Proceedings of the Sixth International World Wide Web Conference*, 1997.

[6] InterCare Consortium, InterCare Common Product Interface Specifications - Functional and Architectural Environment of InterCare Security Server (IC-SS), HC 4011, *InterCare Deliverable D3.2*, pp. 101-127, 1999.