

## ***SPECIAL SESSION ON CERTIFICATION AND SECURITY IN HEALTH-RELATED WEB APPLICATIONS***

### **Call for Papers**

#### **Chairs:**

Dr. Ioannis Apostolakis, National School of Public Health, Dept. of Health Economics, Greece

Mr. Anargyros Chryssanthou, MSc, Data Protection Authority, Auditors Department, Greece

Dr. Iraklis Varlamis, Harokopio University of Athens, Dept. of Informatics & Telematics, Greece

#### **Introduction**

The main issue of concern in health-related applications is the protection of medical data. A patient's profile data is deemed as sensitive data and is protected by data protection laws. Medical data needs to be accessible only by authorized people. It needs to remain confidential, maintain its' integrity, and be available to authorized people upon request. In the classic model of CIA, this perspective publication seeks to integrate two new aspects of security, authorization, and non-repudiation.

In the case of health related web applications, medical information that is transferred across the network should be encrypted, secured, and protected. Additionally, to secure the exchanging endpoints we need to accurately verify the real identity of the exchanging parties, in order to prevent cases of identity theft. Any transfer of medical data also needs to be audited properly, in order for the administrators responsible or the authorities to be able to connect any faulty transaction with the exchanging parties and attribute responsibilities. Processes need to be established to be able to certify each transacting party, each transfer, and the associated level of security. Certification, in terms of security, refers to the compliance to suitable standards and regulations ranging from the ISO 27001:2005 standard to HIPAA and data protection laws. Certification in health-related web applications springs from the need to verify the accurate, impervious, and protected exchange of medical data.

#### **Objective of the Special Session**

This session aims to provide relevant theoretical frameworks and the latest empirical research findings in the area. It is expected to increase interaction between members of the medical community, IT professionals, and all other interested parties. It is also expected to review the certification and security procedures through collaboration, to identify open threats and emerging needs, and to provide solutions. Works presented in the session are expected to cover as many security and certification issues as possible and provide practical solutions and case study applications. This session aims to uncover security and certification issues that lurk in the background and indicate possible solutions.

## **Target Audience**

The target audience of this session comprises professionals and researchers that employ, study, design, and implement health related web applications. Students of management of healthcare systems and healthcare managers in general are encouraged to attend the session since it will help them to avoid design pitfalls and will provide them with a walkthrough towards building trustful medical application. Security professionals working in medical institutions will be able to identify compliance requirements and implement the proper measures to achieve an adequate level of security for medical data and certification, either by certification bodies or by data protection authorities.

## **Recommended topics include, but are not limited to, the following:**

Confidentiality, Integrity, Availability in health related web applications  
Risk analysis in health related web applications  
Medical computer networks and security management  
Applying ISO standards (ISO 27001:2005, ISO 17999:2005) in healthcare environments  
Compliance in health related web applications  
Health related web applications and data protection laws  
Trust in healthcare communities  
Certification in medical applications

## **Submission Procedure**

All papers are peer reviewed by members of the Scientific Committee. If you would like to present your work at the Special Session, and have your paper published in the Conference Proceedings, submit a short abstract (200 words) to [icictth@ineag.gr](mailto:icictth@ineag.gr) (**Mandatory CC** [varlamis@gmail.com](mailto:varlamis@gmail.com)) before **8 May 2009**. Authors will be notified on the acceptance of the abstract by **15 May 2009** and should proceed with submission of the full paper on or before **31 May 2009**.

Extended versions of the papers of the session will be published as book chapters in the book: "Certification and Security in Health-Related Web Applications: Concepts and Solutions" (<http://www.igi-global.com/requests/details.asp?ID=611>) published by IGI Global, after peer revision by members of Conference Scientific Committee and the Book's Editorial Advisory Board.

## **Important Dates**

**May 8, 2009:** Abstract Submission Deadline  
**May 15, 2009:** Notification of Abstract Acceptance  
**May 30, 2009:** Full Paper Submission  
**June 10, 2009:** Notification of Full Paper Acceptance