The 2017 IEEE International Workshop on Healthcare Data Security and Reliability

in conjunction with

QRS 2017

Prague, Czech Republic, July 25-29, 2017

In this current technological era, a huge amount of medical and biological data has been managed electronically and it has demanded the seamless availability of E-health applications anywhere anytime. This demand has paved the ways for modern healthcare technologies deployment in telemedicine and mobile healthcare services. While on the other hand, this rapidly evolving technologies and their deployment in healthcare systems also pose many unseen threats disguised in this technology giant. And these might affect the conducive working environment of a healthcare organization and its smooth processes from patient's data privacy to healthcare records protections and their secure transmission among various healthcare locations. These unseen treats could be due to the vulnerabilities inherited/disguised in any of the technology parameter or service delivery mechanisms that appear with the time after the technology is deployed. Since by the time, the critical healthcare processes would be relying on the newly deployed technology; appearing such issues would affect adversely and become intolerable. Many healthcare organizations have faced numerous loses including public confidence due to these security flaws in recent years. Although the security efforts and technologies have evolved significantly but it still remains a challenging task (due to novel unseen and continuously emerging threats) and requires a continuous struggle to address these issue. The other significant reason is the repeated and sophisticated security attacks that continuously introduce malicious softwares and pose threats to patient's data privacy and healthcare security.

The aim of this track is to provide original and the latest contributions, and to review and survey research and development on information assurance, data privacy and applications security in healthcare systems that would help users to strengthen their security parameters.

The HDSR workshop will be co-located with QRS 2017.

Topics of interest

Topics include, but are not limited to:

- Data storage and management (physical storage & availability issues, maintenance, etc.)
- Healthcare data protection
- Healthcare application's security
- Vulnerability assessment in healthcare systems
- Unified and ubiquitous access (platforms, infrastructures, interfaces) of healthcare systems
- Secure health information exchange based on mobile agents
- Healthcare data/system integrity
- Data security and data privacy for mobile healthcare devices
- Identity theft and related abuses
- Healthcare data security strategies
- Intrusion detection in healthcare care systems
- Healthcare security policies and procedures
- Healthcare data tampering

- Healthcare database security
- Trust management

Format and Proceedings

All submissions must be in English and original works that have not been published and/or submitted for consideration of publication anywhere else. The format of the submission must follow the guidelines for IEEE conference proceedings with maximum of eight pages. Each submission should also include a 150-word abstract and up to 6 keywords.

All accepted papers will be published by IEEE Press and made available in the IEEE digital library as the company of QRS proceedings. Detailed instructions for electronic paper submission and the review process can be found at the QRS17 conference submission website http://paris.utdallas.edu/qrs17.

Important Dates

- April 15, 2017 Submission deadline (extended)
- May 25, 2017 Author notification
- June 5, 2017 Camera-ready dues
- July 25-29, 2017 Workshop

All above deadlines are AOE time.

General Inquiries

For more detailed and updated information, please refer to http://paris.utdallas.edu/qrs17,
or contact Professor Haider Abbas (National University of Sciences and Technology (NUST), Pakistan).