Smart Connected Health Systems (SCHS) connect smart medical devices (e.g., smart wearable devices, medical sensors, and smart medical instruments), electronic medical records, and medical cloud. They are designed to support many life-critical, context-aware, and intelligent medical applications to improve the efficiency and quality of healthcare services, as well as reducing the cost of offering such services. When massive amount of valuable and sensitive data is collected, transmitted, stored, and analyzed in SCHS, securing these data and preserving the privacy of the users are challenging, both in research and in practice. Several features in SCHS, including heterogeneous medical devices and communication channels, resource constrained and unreliable embedded devices, and complicated application logic, further complicate these security and privacy challenges. Although many efforts have been made in designing secure, privacy-preserving SCHS, security and privacy-preserving solutions for SCHS are still at an early stage. In addition to addressing the needs of technology solutions in security and privacy, it is also essential to design and establish new security and privacy policies, and to standardize security and privacy related procedures and requirements.

The aim of the proposed Topical Collection is to promote research and reflect the most recent advances of security and privacy issues of SCHS, with emphasis on the following aspects, but certainly not limited to:

- Mobile Healthcare Security
- Smartphone Security for Healthcare
- Wearable Device Security
- Medical Device Security
- Security and Privacy Issues of Implantable Medical Sensors
- Biometrics
- Wireless Communication Security
- Security and Privacy for Wireless Body Area Networks
- Secure RFID technology
- Secure Cloud Health System
- Big Health Data Security
- Differential Privacy for Health Data
- Secure Machine Learning for Health Data
- Privacy-preserving Big Health Data Analysis
- Novel Threats and Attack Models
- Novel Trust Models
- Security Detection and Evaluation
- Key Management
- Cryptography for Health Systems
- Security Management (administration and training) in Health Systems
- Security in Virtualized Health Systems
- Security Risk Assessment
- Security and Privacy Policies in Health Systems
- Security in Electronic Health Record Systems
- Blockchain and its Application in Healthcare
- Secure Networking in SCHS
- Access control for SCHS

**Submission Guidelines**

Papers must be written in English and describe original research which is not published nor currently under review by other journals or conferences.

Author guidelines for preparation of manuscript can be found at: [http://www.springer.com/public+health/journal/10916](http://www.springer.com/public+health/journal/10916)

To submit, please go to [http://www.editorialmanager.com/joms](http://www.editorialmanager.com/joms) and choose the Article Type "SI: Security and Privacy in Smart Connected Health Systems”

All submissions will be reviewed according to the journal peer-review policy.

**Timeline**

Paper submission due November 30, 2018

Notification of acceptance: January 31, 2019

Final manuscript due: April 30, 2019

*Journal of Medical Systems* participates in the Continuous Article Publication (CAP) workflow, wherein articles that are accepted are published immediately into an issue without an Online First waiting period. If your article is accepted for publication, it will be published immediately into the next available issue, but labeled and sorted into a Topical Collection on Security and Privacy in Smart Connected Health Systems.

**Guest Editors**

Kim-Kwang Raymond Choo
Dept. of Information Sys. & Cyber Security
University of Texas at San Antonio, USA
raymond.choo@fulbrightmail.org

Kewei Sha
Dept. of Computing Sciences
University of Houston – Clear Lake, USA
sha@okcu.edu