Patient data security in the era of medical connected devices

Tudor C. DRUGAN* and Dan ISTRATE

Department of Medical Informatics and Biostatistics, Iuliu Haţieganu University of Medicine and Pharmacy, Louis Pasteur Str., no. 6, 400349 Cluj-Napoca, Romania
E-mails: tdrugan@umfcluj.ro; distrate@umfcluj.ro

* Author to whom correspondence should be addressed; Tel.:+4-0264-597256 int 2501

Abstract
Internet of Things (IoT) is a domain that includes embedded devices connected to a network and used in multiple applications such as: transport, telecommunications, medicine, industrial field and many others. Medical Connected Devices are IoT devices and have their origins in wireless sensor networks and extend this concept by proposing applications in which embedded devices connected to the Internet help automate user tasks. Thus, IoT devices are imagined in multiple applications, from home scenarios (smart home) to clinical scenarios.
Considering that IoT devices impact the medical practice and patient life, there is a pressing need for security mechanisms. Security is considered one of the most important IoT characteristics, but it is not considered a key factor influencing acceptance rate.
Medical IoT devices are an attractive target for attackers, as they operate with private user data and can be used as an attack vector (for example, for DoS attacks). The peculiarity of the IoT context is that a security breach can endanger human lives or privacy, as well as causing economic damage. Another particular feature of the Medical IoT context is the difficulty of designing security solutions, due to the multiple limitations of the devices, including: hardware and software limitations, lack of input-output modules, installation scenarios and more. Given these particularities of IoT devices and adding the multitude of software and hardware platforms, along with the lack of standardization, there is a pressing need for new security solutions.
Without complying with basic cyber security standards, many medical IoT manufacturers focus exclusively on the features of the devices they sell. In many cases, they do not check for vulnerabilities in the final version of the product, nor for the corresponding applications through which the product can be controlled. It could be negligence, but a more likely explanation is that this approach reduces production costs and speeds up product placement. In any case, this affects buyers who are likely to suffer financial consequences or lose sensitive information when hackers start exploiting the flaws.

Keywords:
Data Collection; Medical Device; Internet of Things (IoT); Data Protection