Protecting Information, Personal Data and Privacy in the Medical Sector

Călin MUNTEAN[a,*] and Olimpiu-Ovidiu CORNEA[b]

[a] Discipline of Medical Informatics and Biostatistics, "Victor Babeş" University of Medicine and Pharmacy from Timişoara, Eftimie Murgu Str., No. 2, 300041, Timişoara, Timiş, Romania
[b] Banat's University of Agricultural Sciences and Veterinary Medicine „King Michael I of Romania" from Timişoara, Calea Aradului, no. 119, 300645 Timişoara, Romania
E-mails: cmuntean@umft.ro; cornea.o@gmail.com;

* Author to whom correspondence should be addressed

Abstract
Given the importance of protecting the critical infrastructure of the state of which the Health sector is part, interdisciplinary collaboration in order to obtain fast and efficient results has become a necessity. Considering the impossibility of carrying out any modern medical activity without the support of computer systems, the protection of information transmitted and personal data throughout their lifetime, becomes a task of great responsibility. The legal constraints imposed on the protection of personal data, the guides of good practice in the field and the standards applicable to information protection oblige the continuous training of our own staff to become responsible, highly qualified and well trained. Also, given that most of the malfunctions of a system come from within, the design of future ICN systems and staff training is essential. Fundamentally, the operation of essential infrastructures can be optimized and kept under control by regulatory measures (legislation, standards, accreditations, etc.), by organizational measures (limiting access to information using the principle of need to know, using the rule of two pairs of eyes, using the principle separation, performing real, relevant and periodic risk assessments based on which to implement appropriate measures to treat detected risks, policies, procedures, etc.), through technical measures (use of secure and segmented networks, strong passwords, restriction access to authorized personnel, data backups, monitoring systems as a whole and maintaining logs, implementation of systems such as IDS, IPS, Firewall, Antimalware to prevent and respond to cyber attacks, use of microclimate control equipment , etc). In conclusion, the design of ICN health must take into account the protection of data and information in the medical system as a whole or is essential, can be done effectively following rules and procedures, but requires interdisciplinary collaboration, including doctors, engineers, computer scientists, specialists in risk management, information security specialists.

Keywords: Critical infrastructure; Personal data protection; Information security management; Risk management; Intrusion detection system; Intrusion prevention system; Firewall