PATIENT SAFETY AND CIBER-SECURITY

Ever since the early days of medicine and until some six decades ago, there was much more privacy around patient data and therapeutics. Thanks to the Hippocratic Oath, legal imperatives, motley physician handwriting and others, it was doctors, nurses and archivists who, in the end, were in charge of the compilation and custody of health records.

The industrial age brought with it radical and accelerated changes that defined hospitals and the modern health system. The roles of new actors took shape and their annotations appear reflected in files. These actors include social workers, psychologists, microbiologists, dentists, pharmacists, nutritionists and therapists.

With the evolution of information technologies, digital health records appear, bringing about such benefits as savings in storage space, greater clarity of written information, possibility of creating backups almost immediately, device portability and, also, sensitivity to sharing on networks, both internal and global.

Digital files can simultaneously gather information produced by a clinical laboratory and by studies of medical imagery. Their contents may be used for research and teaching or for sharing at boards of experts, both synchronously and asynchronously.

The huge capacity of IT systems to store and process enormous amounts of data, at high speeds and with great precision, affects the evolution of different areas in society, particularly the economy, government and industry. Control over information brings power and, therefore, conflicts.

Early cases of data theft, manipulation or vandalism of IT systems were not of great concern to health institutions. Attacks were mostly aimed at financial, business, political, industrial and military scenarios. The belief was that no one in their right mind would want to harm ill people.

But it did not take long for computer criminals to realize the value of information stored by the biomedical industry and hospitals. As they explored the territory, they discovered that health centers are not usually well-protected, contrary to the financial, military or business

systems. In many countries, investment in equipment, software and cyber-security is quite delayed, especially in public systems. This shortfall becomes an advantage for those who surf the net wreaking havoc and looting, just like pirates and privateers in the ocean.

Patient safety may be affected at many different levels by cyber-attacks. The most common harm is theft of confidential information, which is later used for purposes of extortion or identity theft, causing patients economic, labor, psychological and social hardship. The legal consequences of this form of crime also take a toll on health organizations, since they may be accused of negligence in the compliance with their legal and ethical duty to safeguard medical record privacy.

Criminal intrusion into computer systems can also lead to total or partial operating paralysis, affecting major components such as appointments, procedures of diverse complexity and urgency, and delivery of medication and other therapy in an accurate and timely manner. These are all serious risks to health and life. Malware could corrupt or delete information, both from records and from other sources, such as scanners, dosing units and monitors.

Each year ever more complex medical devices are brought to market, many of which are implanted in individuals, like pacemakers. These vital devices contain processors or chips that are calibrated and updated by connecting them to specific terminals. Many clinical monitoring machines operate under these same principles and, therefore, could be affected by malicious instructions that make them fail, either immediately, randomly, or on given dates or points in time. Damage could even originate from an attack to the manufacturing plants of primary components required for assembly.

The reasons for targeting a hospital or health system are diverse. Aside from intrusions that aim to obtain an economic benefit, other reasons go as far as morbid curiosity, perverse intention to cause harm, or desire for notoriety. In fact an attack aimed at totally different objectives could spread through hospital networks, harming records, systems, applications and hardware.

The global geo-political paradigm cannot be ignored either, because many countries and terrorist organizations have cyber-war divisions that are continuously testing technologies

and strategies in an effort to access and paralyze the resources of their enemies. Unfortunately, one of these strategic targets is health services.

Back in the 1960´s, the word "*hack*" referred to finding an optimal and sophisticated solution to an IT issue. The term *hacker*, linked to an individual who causes damage to information systems, appeared in 1963. Not until 1980 were the first laws enacted in the United States and England penalizing the criminal use of computers and software.

In 2016, the United States experienced a criminal intrusion of the IT systems of three hospitals. The hacked information, data of thousands of patients, was put up for sale on illegal websites. That same year, similar attacks were reported at German and Austrian hospitals.

More recently, in May 2017, some twenty-five hospitals in England suffered a ransomware attack. Attackers resorted to malware and requested payment in exchange for, allegedly, restoring access to clinical data. Besides affecting the care of inpatients and outpatients, the operation of ambulance services was also impacted. In this particular case, the possibility of theft of confidential data cannot be discarded.

The security of contemporary healthcare services requires a permanent effort to ensure the optimal and adequate functioning of hardware and software and of all computer-operated devices involved in patient safety and security. Protocols and standards must be continuously kept up to date and observed, and possible vulnerabilities must be anticipated in order to ensure a more timely response to new circumstances. Healthcare service security must be in the hands of a team of experts, constantly updated, in compliance with specific and modern national policies. Not taking action against cyber threats is an inexcusable negligence that could lead to harm of an unimaginable magnitude.

Planning and organization to quickly address an attack, and the continuous management of system security, are challenges for society at large, laws, healthcare systems and health professionals as part of their duty to strengthen patient safety and security.

Dr. Robinson Rodríguez Herrera

Institutional Patient Security and Quality Program

(Programa Institucional de Calidad y Seguridad del Paciente)

CCSS – Costa Rica

National Children Hospital of Costa Rica

Universidad Santa Paula – ULACIT

drrobinsongerenciasalud@gmail.com

Publicación original en español: http://www.dgdi-conamed.salud.gob.mx/ojs-conamed/index.php/BCCCSP/article/view/721/0

http://www.dgdi-conamed.salud.gob.mx/ojs-conamed/index.php/BCCCSP/article/view/721/0