"Security in Healthcare.
Personal data protection: procedures and responsibilities."

- November 21, 2017 –

Electronic Medical Records are the most popular target for cybercrime due to the presence of confidential data which includes: basic identity information, contact information, billing information, patient medical history and more. Medical and financial organizations are the fields most vulnerable to attacks, such as ransomware, which on a global level was near 40% in 2016[1]. These industries are among the most dependent on electronic information, therefore are the first hackers focus on due to the lack of detection technology and daily record backups, among other vulnerabilities. The average ransom for data decryption has increased by 3 since 2014 (from $373 in 2014 to $1077 in 2016), and 72% of institutions infected by ransomware lost access to their data for over 2 days. Losses, on a global scale, caused by ransomware are projected to be over 5 billion dollars in 2017.

According to "2014 Data Breach Category Summary", medical records are the most advantageous target for Cybercrime by hackers, representing 43% of total attacks[2]. The main challenge lies in increasing the level of data protection without hindering the rapidity at which lifesaving information can be accessed by healthcare professionals.

Cyber risks for medical organizations may be:

- Identity theft resulting in the loss or theft of data from medical records;
- E-vandalism;
- Security breaches in medical health records;
- Business continuity risks due to security mechanisms or viruses;
- Cyber extortion;
- High costs due to security notifications, crisis management, and disaster recovery solutions.

Major repercussions are expected within the field of specialized medical applications, particularly in the area of Big Data, Cyber Disaster Recovery, Mobile Computing, Data Loss Prevention, as well as those implicated in controlling access and application vulnerability.

From a European perspective, 74% of Europeans consider medical information to be personal information. In Romania, only 50% consider medical information to be personal information.

From the standpoint of EU regulations concerning the protection of personal data (General Data Protection Regulation-GDPR), medical information is regarded as special

[1] https://www.malwarebytes.com/surveys/ransomware

[2] http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2014.pdf

category of data, as any patient has the right to request a copy of their personal data for their individual use. If the patient submits the application by electronic means only, the information may be provided in the electronic format most widely used, for example a common file, PDF or any other format for general use. According to the GDPR, the patient is also entitled to manage or transfer their own electronic medical records, therefore the Data Protection Operator (DPO) has the obligation to safely provide patient information in a standard electronic format that is widely and commonly used. Additional costs from the implementation of changes due to the GDPR may not be charged to the people concerned, nor shall they be able to be used as justification for refusal to respond to requests of data portability.

What is the GDPR (General Data Protection Regulation)?

The European Parliament adopted the GDPR in April 2016. It carries provisions that require businesses to safeguard personal data and the privacy of EU citizens in transactions that occur within EU Member States. It also regulates the export of GDPR personal data outside of the EU. Provisions are applied in all 28 EU Member States, in order to implement a set standard throughout the EU.

Any company that stores or processes personal information regarding EU citizens from EU countries must respect GDPR, even if even if not present within the EU. The specific criteria for companies that must comply with are:

- A presence in an EU country;
- No presence in the EU, but it processes personal data of European residents;
- More than 250 employees;
- Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data.

This effectively means almost all companies are obligated to be in compliance starting May 25, 2018.

Regarding costs necessary to comply with the requirements of the GDPR, a PWC survey of U.S.-based companies reported that 68% of said companies expect to spend $1 million to $10 million USD to meet GDPR requirements. Another 9% expect to spend over $10 million USD[3].

[3] https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

What happens if my company is not in compliance with the GDPR?

The GDPR allows for steep penalties of up to €20 million or 4% of global annual turnover, whichever is higher, for non-compliance. According to a report from Ovum, 52% of companies believe they will be fined for their failure to fulfill the GDPR's obligations[4]. Management consulting firm Oliver Wyman predicts that the EU could collect up to $6 billion in fines and penalties in the first year.

GDPR quick sanctions allows up to 20 million or 4% of total annual turnover, whichever is greater, for failure to meet obligations. According to a report of the company Ovum 52% of companies, believes that they will be fined for failure to fulfil obligations. Management consulting firm Oliver Wyman says that the EU could collect up to $6 billion in fines and penalties in the first year.

What types of privacy data does the GDPR protect?

- Basic identity information such as name, address and ID numbers;
- Web data such as location, IP address, cookie data and RFID tags;
- Health and genetic data;
- Biometric data;
- Racial or ethnic data;
- Political opinions;
- Sexual orientation.

[4] https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html?page=2