"Security and standardization in health.
How prepared are we for GDPR implementation in May 2018?"
- March 6, 2018–

The European Parliament adopted the General Data Protection Regulation (GDPR) on April 14, 2016, but its provisions become applicable in Romania after a two-year implementation period, more precisely as of May 25, 2018. The regulation is not a Directive and therefore does not need to be doubled by national law, its provisions being directly applicable from the date set.

The main provisions of the new legislation clarify the rights of individuals on personal data, as well as obligations on data storage and processing by data processors. At the same time, it is clearly stipulated that medical data is personal data of a special nature and, therefore, benefit from differential treatment. Regarding the awareness of the need to implement GDPR, 74% of Europeans and only 50% of Romanians consider that medical information is personal information.

According to the GDPR, any patient needs to be informed and agree on how and why his/her personal data will be processed. The patient has the right to request a copy of the personal data that is being processed. Information can be provided in a commonly used electronic form, which means a common, PDF file or other general purpose format. The patient benefits from the right to "be forgotten", that is, may require that his or her personal data be no longer used in the processing, even if originally agreed. The regulation provides for the right to data portability, i.e. the patient can transfer his/her medical records to another data processor. In this regard, the data processor has the obligation to provide the patient with the information in a standard, open and commonly used electronic format.

It is important to underline that the provisions of the Regulation apply to all data processors, regardless of their origin, as long as they process personal data of European citizens. Costs incurred by implementing changes made by GDPR will not be attributable to the data subjects nor can they be used as a justification for refusing to respond to data portability requests.

In order to ensure the protection of personal data, data processors must take measures to limit undue access to them. The main challenge is to increase the level of data security without hindering the rapid access of healthcare professionals to potential information that can save patients' lives.

Medical records are the most attractive target for cybercrime due to the presence of confidential information in the same place, such as identity information, contact details, billing data, medical history. Some data protection risks in medical organizations are described below:

- Identity theft resulting from the loss or theft of data from medical records
- E-vandalism - personal data loss or exposure due to lack of or non-compliance with specific procedures
- Security breaches in health records
- Business continuity risks due to non-implementation of security mechanisms or virus activity
- Cyber extortion - stolen or encrypted data ransom requests
- Costs associated with security audits, crisis management, and disaster recovery solutions

At the level of computer systems used by data processors, major implications are expected in specialized medical applications, especially in the area of:

- Big Data
- Mobile Computing
- Access control
- Data Loss Prevention

Medical institutions are among the most vulnerable areas of cyber-attacks, being among the most dependent on electronic information. Therefore, they are first to the attention of the attackers, knowing that they do not have the technologies necessary to detect the attacks or back up for the relevant data to date.

The application of GDPR by healthcare providers will provide the opportunity to identify security risks and reduce exposure to these risks at the level of the whole Romanian medical system by implementing clear policies and methodologies to ensure that patients' rights are complied with and to take into account the obligations of data processors.

To this end, each organization must be aware of and define at the management level the steps to be followed. They can also be defined and grouped (on a general level) as follows:

- preparatory steps – e.g. auditing the existing situation, appointing the data protection officer, defining the working methodology, identifying the risks and methods of reducing them, defining the specific procedures of the organization, etc.
- implementation steps – e.g.: staff awareness on the need for GDPR, training of staff on procedures specific to each work point, purchase of physical and cybernetic protection equipment, etc.
- maintenance and improvement steps – e.g.: monitoring compliance with established procedures, ongoing audit of processes within the organization to identify new emerging risks, correcting procedures specific to each work point to eliminate identified risks, etc..

The implementation of the new provisions requires broad training covering both the public sector and the private sector of healthcare providers, both in terms of workflows and by the use of computer systems.

What does GDPR (General Data Protection Regulation) mean?

The European Parliament adopted GDPR in April 2016. It provides for provisions requiring businesses to protect personal data and the privacy of EU citizens for transactions taking place in EU Member States. GDPR also regulates the export of personal data outside the EU. The provisions are applied in all 28 EU Member States, with only one standard.

Any company that stores or processes personal information about EU citizens in EU states must adhere to GDPR even if they do not have a presence within the EU. Specific criteria for companies that need to comply are:

- Presence in an EU country.
- No presence in the EU but process personal data of European residents.
- More than 250 employees.
- Less than 250 employees, but data processing affects the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data.

This basically means almost all companies. As of May 25, 2018, the provisions are mandatory.

Regarding the cost of complying with GDPR requirements, for example, according to a PwC[1] study, 68% of US companies are expected to spend between $ 1 million and $ 10 million, and 9% expect to spend more than $ 10 million.

What happens if my company does not comply with GDPR?

GDPR allows rapid sanctions of up to € 20 million or 4% of global annual turnover, whichever is greater, for failure to comply with the obligations. According to an Ovum[2] report, 52% of companies believe they will be fined for non-compliance. Management consulting firm Oliver Wyman believes the EU could collect up to $ 6 billion in fines and sanctions in the first year.

What types of privacy data protects GDPR?

- Basic identity information such as name, address, and identification 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

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

National Interoperability Framework (NIF - adopted by Government Decision no. 908/2017) will regulate how the interoperability of information systems in public administration in Romania and between it and EU systems can be ensured, reducing the number of redundant data sources in public administration and increasing the capacity to provide inter-institutional data *by using standard data formats*. *The NIF will regulate a number of common rules on electronic data transfers* between public authorities and institutions, as well as between them and the citizen, respectively the business environment or the representatives of civil society.

Taking into account the development of ICT in public administration, the priorities for the National Digital Agenda Strategy for Romania 2020 in line with the Strategy for Strengthening Public Administration 2014-2020, *it is necessary to achieve a single government policy and* ***common standards*** *in the entire public administration in the IT field*.

The main change in government policy through the adoption of the NIF is *the single centralized perspective on their IT systems and interoperability functionality*. This implies that *each public authority or institution will be obliged to observe, when purchasing IT&C products or services, a minimum standard of interoperability* that will enable ***the exchange of standardized data*** with other information systems of other public authorities or institutions in the near future. The transfer of information will be done at predetermined times, without the intervention of staff, which will also reduce the administrative burden and eliminate human errors. This policy will primarily ensure compliance with the principles laid down at European level, principles guaranteeing a minimum standard of quality in public services offered to citizens and the business environment such as inclusion and accessibility, *security and confidentiality of information*, multilingualism , transparency, administrative simplification.

Corresponding to the 7 piers underlying the Digital Agenda for Europe 2020, Romania has defined four areas of action including:

- ✓ **Area of Action 1 - eGovernance, *Interoperability, Cyber Security*, Cloud Computing, Open Data, Big Data and Social Media** – increasing efficiency and reducing costs in the public sector in Romania by modernizing the administration.
- ✓ **Area of action 2 - ICT in education, *health*, culture and inclusion** – intervenes in the social challenges at the sectoral level and ensures that ICT investments will have a positive impact in the social context.