BioSpectrum the business of Bio & Health Sciences

How GDPR will specifically affect healthcare?

18 May 2018 | Features | By Rajesh Maurya

GDPR enacts stringent protection and processes for handling particular types of PII medical information. In general, an organization may collect and process personal medical information only if it is necessary for patient treatment and diagnosis, and with the explicit consent of the patient.

The European Union's General Data Protection Regulation (GDPR) will begin May 25, 2018, and businesses across the globe are bracing for the updated legislation. The GDPR is changing more than data compliance—it's changing the way businesses operate—affecting how and when they interact with the data of EU residents. One industry that will be held to higher standards is healthcare.

The healthcare industry can expect a variety of new challenges when it comes to gathering and protecting the personal data of European Union residents. The new legislation aims to build upon common and current personal information protection, working to ensure that data is protected across all processing activities and endpoints.

A Closer Look at the General Data Protection Regulation

The GDPR is a fundamental shift in the protection of an individual's data and privacy. Prior to this legislation, personal data was widely viewed as the property of the businesses who collected and stored the information. In May, however, any personal data of European Union residents will be seen as the individual's property, and the GDPR provides rights regarding the access and usage of their data by organizations. At its core, the GDPR defines the rights of the individual as they relate to data protection. These rights can be broadly summarized as follows:

- **Informed Consent**: The right to be clearly informed why the data is needed and how it will be used. Consent must be explicitly granted and can be withdrawn at any time.

- **Access:** The right to access, free of charge, all data collected, and to obtain confirmation of how it is being processed.

- **Correction:** The right to correct data if inaccurate.

- **Erasure and the Right To Be Forgotten (RTBF):** The right to request erasure of one's data.

- **Data Portability:** The right to retrieve and reuse personal data, for own purposes, across different services.

GDPR also introduces a new obligation on organizations to notify relevant authorities of any personal data breach likely to result in a risk to "the rights and freedoms of individuals". Where that risk is deemed 'high', notification must also be extended to the affected data subjects. Notifications must be made 'without undue delay' and where feasible, within 72 hours of the event discovery. Note, one way to ensure that a breach would not likely result in a risk to EU resident data owners is to encrypt all collected personal data. If this strategy is pursued, organizations need to consider their ability to support large amounts of encrypted traffic in transit and at rest.

The GDPR acts as a means of protecting personal data for EU residents across the globe. This means that any business or organization that processes or stores the data of EU residents are subject to GDPR rules and regulations—regardless of whether the healthcare facility physically operates in European Union countries.

For United States-based healthcare organizations, the GDPR can be seen as an expansion of the Health Insurance Portability and Accountability Act's (HIPAA) regulations. Similar to the protection HIPAA provides for personal health information (PHI), the GDPR expands on the notion by regulating the entire life cycle of personal information, including how its gathered, processed, stored and ultimately destroyed.

How Can Healthcare Organizations Comply with the GDPR?

In order for healthcare organizations to comply with the GDPR, there are a number of requirements, some healthcare specific, that must be adhered to. All "personal data," defined as "any information relating to an identified or identifiable natural person," has to be gathered in accordance with Article 5 of the GDPR, meaning data must be:

- Collected for specified, legitimate and explicit purposes and not processed in a way which is incompatible with them.
- Processed lawfully, fairly and in a transparent manner.
- Processed to ensure appropriate security of data.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.
- Controlled by a controller who is responsible for the data and able to demonstrate compliance.

As mentioned earlier, healthcare organizations have a unique set of higher standards to adhere to. Specifically, certain personal data—known as genetic data, data concerning health and biometric data—can't be processed unless it falls into certain categories. Before we dive into what those categories are, we should define the three types of healthcare-related personal data subject to the specific regulation.

Genetic data: *personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or health of that natural person and that result, in particular, from an analysis of a biological sample from the natural person in question.*

Data that concerns health: *personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.*

Biometric data: *personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.*

While the GDPR prohibits the unnecessary collection of personal data by healthcare organizations, there are several exceptions that allow for its collection. In order for healthcare organizations to collect specific personal data, the collection has to fall into one or more of the following categories:

1. *Data has been given with explicit consent from the owner*
2. *Processing data is necessary to the "vital interests" of the patient/provider*
3. *Processing is needed for the purposes of preventative or occupational medicine*
4. *Data is necessary for the good of the public health*

What are the Penalties for Non-Compliance?

Failure to comply with the GDPR can mean serious fines for healthcare organizations. Fines are calculated based on a number of factors but can range up to the greater of €20 million ($24.8 million) or four percent of global annual turnover. The word "greater" here is important. If compliance failure or a data breach is discovered and penalized, the higher-generating sum at the time of the fine will be used. This means that if four percent of global income for the healthcare organization was higher than 20 million Euros, the fine would be the amount equal to four percent of global income.

How Can Healthcare Facilities Brace for the GDPR?

If your healthcare facility finds itself having to meet GDPR requirements this spring, there are several actions you should be taking to help ensure that you're prepared:

First, you should audit your facility to determine the personal data that needs to be reorganized for compliance. Make sure you include insight into what data is collected, how its collected and the purpose for collecting the data.

Second, ascertain how the data is being processed, stored, transferred and shared inside/outside your facility. Organize and consolidate any possible information silos to ensure that the necessary information isn't being lost in badly implemented processes or technologies.

Once you've audited information protected under the GDPR, you should invest in educating and training staff on the revised data life cycle requirements; updating the procedures for gathering, using, storing and destroying personal information. In addition, data security and privacy teams need to be prepared should any information be audited or requested by an EU resident.

Next, you should review your cybersecurity capabilities. Determine if your organization is capable of detecting and reporting data breaches within the required 72-hour window. Breach detection is very difficult, even for the largest enterprises. In fact, the majority of data breaches is detected by third parties – usually by customers or law enforcement. If it can't, you should update your cybersecurity capabilities to help protect your organization against breaches across the attack space.

Finally, you should commit your organization to rigorous risk-based cybersecurity program characterized by continuously assessing your GDPR relevant data life cycle and the organization's overall security posture. While compliance does not necessarily mean secure, given the heavy fines associated with the GDPR, consistently checking for weaknesses within your organization ensures a strong foundation for response should an EU citizen request his or her information, submit a complaint or, worst-case scenario, if sensitive data has been breached.

Rajesh Maurya, Regional Vice President, India & SAARC, Fortinet