NEW EU DATA PROTECTION REGULATION POISED TO CHANGE DATA PRIVACY LANDSCAPE

The bold digital clock featured on the EUGDPR (EU General Data Protection Regulation)[1] website indicates – to the second – the countdown to the regulation's May 25, 2018 enforcement date. The site communicates the sense of urgency and importance of the initiative which it heralds as "the most important change in data privacy regulation in 20 years".

With data breaches among top-tier multinational corporations in the news on virtually a daily basis – and the increasing sophistication in hackers' ability to infiltrate even the most sophisticated security "fences" – the pharmaceutical industry is vulnerable to leaks of the most sensitive, nature: those concerning citizens' personal data.

GDPR BACKGROUNDER

The GDPR applies to all organizations that provide goods and services to people in the EU, although EU Member States may maintain or introduce further conditions, including limitations, regarding the processing of genetic data, biometric data or data concerning health.

It was adopted by the EU Parliament in April 2016 and has been in transition for the past two years. Unlike a directive, it doesn't require legislation to be passed by government. The new regulations replace the Data Protection Directive established in 1995 at a time when privacy wasn't the top-of-mind hot button issue it is today.

The objectives of the GDPR are to: 1) to harmonize data privacy laws throughout Europe; and 2) to safeguard individuals' privacy. Personal information obtained from someone in the EU cannot be processed unless there is a clear legal basis for doing so.

WHAT ARE THE THREE KEY CHANGES?

The GDPR encompasses three key areas: expanded territorial scope, increased penalties for infractions and improved patient consent measures.

1. Expanded territorial scope

The GDPR provides a more clearly defined and expanded definition of the territory it governs. Under the previous guidelines, data privacy jurisdiction was vague and the ambiguity of the language left it open to interpretation and litigation. The scope of the GDPR is broader than before. The new rules apply "to all companies processing the personal data of data subjects residing in the European Union, regardless of the company's location". It extends to controllers and processors outside the EU whose processing activities relate to the offering of goods or services to, or monitoring the behavior of, EU data subjects (within the EU). For non-EU based organizations, it's important to bring on a subject matter expert who can advise on the implications of the GDPR and how it will affect business operations.[2]

2. Increased penalties for infractions

Non-compliance with GDPR regulations may result in substantial fines totaling up to 4% of the company's global revenues or €20 million, whichever is greater. This is the highest possible fine imposed for the most serious type of non-compliance, such as lack of sufficient customer consent to process data, or violating key "privacy by design" concepts. This stipulates that businesses must consider data privacy from the outset of the design of a project, as well as throughout the lifecycle of the relevant data processing. This means integrating data privacy processes at the initial conceptual stage, rather than "retrofitting" them later.

The penalties for non-compliance exist on a sliding scale, depending on the seriousness of the infraction.

3. Improved patient consent measures

As part of the GDPR, the language of consent will be made more accessible to the lay public. It must be written in clear and plain language, and withdrawal of consent must be simple.

IMPACT ON THE PHARMACEUTICAL INDUSTRY

The key question is, what does all this mean for clinical trials and data collection?

The GDPR applies to personally identifiable information (PII). This is information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context. It concerns pharmaceutical manufacturers, contract research organizations (CROs) and software/application vendors operating in the EU, including companies that are already compliant with HIPAA (the Health Insurance Portability and Accountability Act).

The new regulations will have a far-reaching impact on the medical research sector. The implication is that if a U.S. pharmaceutical manufacturer or biotech company is conducting a trial in Switzerland, for example, the patient data gathered must adhere to the laws set out in the GDPR. On the other hand, data relating to EU citizens that are transferred outside the European Economic Area (EEA) must be protected "in a manner that is consistent with how personal data is protected in the EEA"[2].

The EEA stipulates the following: personal data are to be kept for a period no longer than necessary for carrying out the purpose for which they were collected. The data processed must be up to date, adequate, relevant and not excessive for the purpose of processing which must be determined in advance of collection. Unless a change of purpose is explicitly authorized by internal rules, the purpose of processing may not be altered subsequently. As well as ensuring that data are up to date, the data controller must allow data subjects to access their data. Data transfers are subject to certain conditions depending on the status of the recipient. The EEA Data Protection Officer keeps a public register of processing operations, based on notifications received from data controllers. This register enables data subjects to find out which administrative entity is keeping what information about them.[3]

IMPLEMENTING SOLUTIONS IN RESPONSE TO THE GDPR

New compliance measures

Clinical trial sponsors will need to carry out a data protection impact assessment, most likely both for trials starting after May 25, 2018, for those that are ongoing and for data that are being processed at that date. This assessment must include:[2]

- A description of the processing operations and the purposes of processing
- An assessment of the necessity and proportionality of the processing
- An assessment of the risks to the rights and freedoms of clinical trial subjects
- The measures used to address those risks

Conforming to the GDPR will mean a change in supply chain processes, specifically, data processing and handling systems.

One approach to safe information exchange is credentials validation – knowing who is logging into information. This would mean gathering personal information, which could include photo identification, a thumbprint and iris scan, recording a driver license or passport number, and verifying personal information such as age and address.

Other options are clinical data de-identification and anonymization. The criteria for these are clear for simple cases, such as data collection using an eCRF (electronic case report form). CROs can automatically de-identify the patients' data at the site, offset dates of birth and redact sensitive data.[4]

De-identification involves removing or recoding health information that could identify an individual such as patient identifiers or references to dates. In data anonymization, all links between the de-identified datasets and the original datasets are destroyed. However, anonymizing personal information such as names, addresses and dates of birth would mean, for example, having to guess at a person's age, which may not provide the accuracy required in a clinical trial setting.

The transmission of non-CRF data is more complicated. These are the data collected from such processes as imaging, ECGs and blood tests. These data typically aren't directly input into the eCRF, but are sent out for expert analysis. They contain sensitive information necessary to the scientific value of the study. Compliance in these situations involves identifying methods used by hospitals, medical device companies and software vendors.

Data redaction may be another option, but may not always be the best solution. Additional security measures include the pseudonymization and encryption of personal data; the ability to ensure ongoing confidentiality; and a process for regularly testing, assessing and evaluating the effectiveness of measures for ensuring the security of the processing.[5]

Steps the pharmaceutical industry can take

Awareness: Every level of the organization must be made aware of the key elements of the GDPR and the changes it signifies.

Knowledge of data subjects' rights: According to the GDPR, every EU citizen possesses carefully defined rights, including:[2]

- **The right to be informed** – data controllers ***must inform*** data subjects when their personal data have been obtained
- **The right of access** – data controllers ***must disclose*** to data subjects why their personal data were obtained and how it is being used
- **The right to rectification** – data subjects will have the right to rectify inaccurate personal data from the controller in the event private information has been processed incorrectly
- **The right to erasure or the right to be forgotten** – data subjects will have the right to erasure when their personal data have been processed unlawfully
- **The right to restrict processing** – in the event the accuracy of personal data is contested, the data subject can have their private information restricted by the controller

The company must appoint a Data Protection Officer who will inform their organization about its obligations under the GDPR, monitor compliance with it, provide guidance and act as a point of contact with regulators.

Organizations conducting clinical trials should maintain documents demonstrating their compliance with the GDPR, as well as data subjects' consent. These documents should be contained in the trial master file.

If a data breach occurs, the controller must report it to the authorities as soon as possible and no later than 72 hours following discovery of the breach.

MOVING FORWARD WITH THE GDPR

While the GDPR's expanded scope increases patient privacy, the new regulations will make it difficult for companies to obtain the data needed and to share it holistically with the researchers who need to interpret it.

In light of the fact that the GDPR is changing the healthcare landscape and clinical trial governance, industry leaders may consider advocating or lobbying for inclusion in the future development of regulatory guidelines and their enforcement. Adopting a proactive stance that encourages collaboration between regulators and pharmaceutical organizations may promote greater industry compliance. It may also help prevent a situation in which healthcare organizations are not clear on what changes are needed and how to implement them, or don't have sufficient time to make the necessary changes.

At Six Degrees Medical, we understand the importance of keeping up to date with regulatory changes that impact how healthcare organizations do business. The laws affecting the pharmaceutical industry are evolving – and our knowledge base is evolving with it. We advise leading pharmaceutical companies around the world, who rely on us for marketing insights that translate into effective tactics. Our passion, creativity and expertise enable us to produce customized medical and scientific communications tailored to client-specific objectives.

Visit us online at https://www.sixdegreesmed.com/ for other industry articles and blogs.

References

1. www.eugdpr.org
2. http://www.clinicaltrialsarena.com/news/data/5-things-to-know-about-gdpr-5934932
3. European Environment Agency: Data Protection at a Glance. Version 1 – December 2010.
4. https://www.clinicalleader.com/doc/pharma-not-prepared-for-new-eu-data-protection-regulation-0001
5. https://www.taylorwessing.com/globaldatahub/article-health-data-privacy-under-gdpr.html. Accessed March 29, 2018.