Considerations for Compliance with the EU General Data Protection Regulation (GDPR):

A Medical Information Contact Center Service Provider Perspective

Larry J. Davis, PharmD,
Vice President Medical and Clinical Affairs

EVERSANA™

eversana.com

EVERSANA™

As we are all well aware, the General Data Protection Regulation (GDPR) establishes a legal framework that sets guidelines for the collection and processing of personal information from individuals residing in the European Union (EU). In the twelve months leading up to the May 2018 deadline for implementation of the GDPR, our medical communications team put a plan in place for our Medical Information Contact Center to ensure full compliance with GDPR in support of our clients. A team of subject matter experts consisting of our internal legal counsel, information technology and business process experts, business unit managers and operational staff, along with an expert external GDPR consultant team, conducted a gap analysis to assess our compliance and ensure our readiness to meet this challenge.

UNDERSTANDING THE GDPR

The first step in our process was to ensure a thorough understanding of the GDPR including all of its key compliance provisions and obligations, understanding its terminology, and answering a key question –"Are we a data controller or a data processor?" A data controller (or controller) as defined under the GDPR is an organization (or natural person) that alone or in collaboration with others, defines what should happen with any personal data that it may collect. A data processor (or processor), on the other hand, is any organization (or natural person) that processes personal data on behalf of a controller. As a service provider, EVERSANA is then clearly a data processor processing personal data on behalf of its clients. Both controllers and processors need to be compliant with GDPR and compliance is, therefore, a shared obligation. The principles relating to the processing of personal data as outlined in Article 5 of the GDPR apply equally to the data processor and the data controller; however, the controller is the decision-maker for how and why personal data are used.

It is important to recognize that within the GDPR, personal information is defined as any information relating to an identifiable natural person (often referred to in the GDPR as a "data subject") by reference to an identifier. Data subject personal information identifiers are similar to what the U.S. HIPAA Privacy Rule calls protected health information (PHI), however, GDPR is inclusive of PHI and at the same time much broader than the HIPAA requirement. The GDPR calls this personally identifiable information (PII) and includes such things as "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR Article 4).

Importantly, the GDPR conveys rights to data subjects (Articles 12 – 23) regarding the handling of their PII. Central to these data subject rights is the right to access their own personal data. From this follows the right to rectification (correct inaccurate PII), right to erasure (right to be forgotten), right to restriction of processing, right to data portability, and right to object to processing in certain circumstances.

FUNDAMENTAL OBLIGATIONS FOR GDPR COMPLIANCE

We identified several key obligations for GDPR compliance that are important to highlight. The first, and most essential requirement, is having in place a privacy policy. Companies must be transparent about how they process and use the data collected from a data subject by giving the data subject access to a privacy statement. The privacy statement should include, among other things, purposes for which the company intends to use or process personal data, the legal basis for processing, the data subject rights, and information about how personal data are kept secure.

Next, the GDPR requires that a company conduct a data mapping exercise with ongoing review and assessment based on any changes in impacted systems and processes. Through data mapping the company must identify where their data are coming from, where their data are actually stored, where those data flow to and from and what is actually being done with those data. Taking the example of a medical information system (MIS) inquiry database it becomes clear that this is not an easy task – it's complicated. First the inquiry comes in through various channels including phone, email, CRM, fax, etc. This alone will take some time to analyze. Let's take for example phone inquiries – who is the vendor for your phone system and software (what information if any do they have access to or control of), do you maintain recordings and if so for how long, where are the recordings stored, are the data kept on mirrored servers, do you have backup data tapes, are your servers outsourced to a vendor or managed by your company IT department, etc.? All data systems will need to be evaluated in this way and the process documented.

Compliance with vendor relationships under GDPR (Article 28) is another key obligation. Controllers and processors must ensure that their respective vendors (those that would be considered sub-processors of

"Companies must continue to ensure compliance with privacy standards that meet or exceed the demands of the highly technical digital world that we live in. The patients, consumers, and health care professionals we all serve expect that we will handle their personal information carefully and that we will keep their data secure, safe and private."

personal information) meet the technical and physical requirements to access and process regulated data. This is accomplished through qualification and ongoing vendor audits, development of compliant vendor contracts and by establishing Data Processing Agreements/Addendums (DPAs) that will be agreed to by your vendors.

Lastly, and perhaps the most challenging for companies (controllers) working in the life science industries, is the obligation to determine the legal basis for processing of PII. Life science companies must address the "Lawfulness of Processing" from Article 6 and the "Processing of Special Categories of Personal Data" outlined in Article 9. As with all aspects of GDPR compliance, this determination is not straightforward and individual life science companies must rely on their own legal counsel and GDPR experts to make these decisions. Under Article 6 will you use explicit data subject consent, or is the legal basis ensuring compliance with a contract or legal obligations, necessary for performance of a task carried out in the public interest, or necessary for the purposes of the legitimate interest, etc.? Similarly under Article 9 is the legal basis for processing explicit consent, or is processing necessary for reasons of substantial public interest, necessary for purposes of the provision of health or social care or treatment or management of health, necessary for reasons of public interest in the area of public health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, or other basis outlined in Article 9?

CONCLUSIONS

GDPR compliance remains a challenge for life science companies and services providers alike. Understanding and implementing compliance obligations under the GDPR is only the beginning. Ongoing review and assessment is important as companies grow and expand to include new business opportunities, implement new systems and/or establish new practices and processes. Some U.S. companies may determine that they have no exposure to GDPR; however, websites, 800 numbers and other available U.S. contact information may attract inquiries from EU residents who are then entitled to the same privacy rights called for in the GDPR. It is also important to keep in mind that GDPR applies to more than just 'customers' – the regulations apply equally to company employees residing in the EU including all of their records and other information accessible by human resources and other departments.

Companies must continue to ensure compliance with privacy standards that meet or exceed the demands of the highly technical digital world that we live in. Privacy regulations similar to GDPR are anticipated to be enacted in California next year, and other states are in the process of developing new privacy regulations as well. The patients, consumers, and health care professionals we all serve expect that we will handle their personal information carefully and that we will keep their data secure, safe and private.