Post-Marketing Pharmacovigilance

The requirements for marketed pharmaceutical products present challenges for companies integrating GDPR legislation into their pharmacovigilance processes

Emma Boulton and Dora Amene at PIPA

European legislation requires that marketing authorisation holders (MAHs) should have an appropriate system for pharmacovigilance (PV) in place. Since the introduction of the updated legislation in July 2012, a set of guidelines for the conduct of PV has been developed by the EMA, known as good pharmacovigilance practice (GVP) modules, to support its implementation (1-4). Each GVP module covers one major PV process. The obligations are the same regardless of the MAH size or if the MAH is an innovative or a generic pharmaceutical company. However, the legislation and regulations do not stipulate how the MAH fulfils these obligations. It is up to the individual MAH to interpret the legislation and regulations and present, at audits and inspections, a system that complies with the requirements. Conveniently, the GVPs break these requirements into topics:

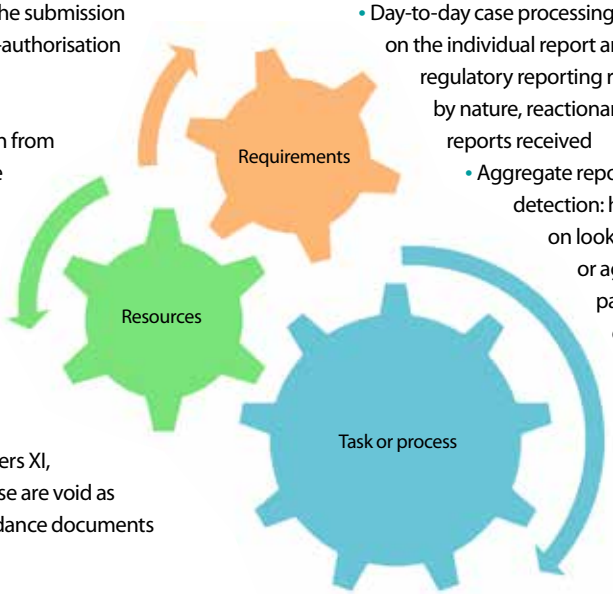
- PV systems and their quality systems (Module I)
- PV system master file (Module II)
- PV inspections (Module III)
- PV audits (Module IV)
- Risk management systems (Module V)
- Collection management and submission of suspected adverse reactions (Module VI)
- Duplicate management of suspected adverse reaction reports (Module VI, Addendum I)
- Periodic safety update reports (Module VII)
- Post-authorisation safety studies (Module VIII)
- Requirements and recommendations for the submission of information on non-interventional post-authorisation safety studies (Module VIII, Addendum I)
- Signal management (Module IX)
- Methodological aspects of signal detection from spontaneous reports of suspected adverse reactions (Module IX, Addendum I)
- Additional monitoring (Module X)
- Safety communications (Module XV)
- Risk minimisation measures selection tools (Module XVI)
- Educational materials (Module XVI, Addendum I)

The eagle-eyed will have spotted the numbers XI, XII, XIII, and XIV are missing from the list; these are void as the planned topics are covered in other guidance documents on the EMA website. The GVPs are living documents that have evolved based on feedback and questions that the EMA receive from MAHs.

Fulfilling the Legal Requirements

The regulations state that the MAH should be responsible for continuously monitoring the safety of its medicinal products, for informing the authorities of any changes that may impact on the marketing authorisation, and for ensuring that the product information is kept up to date. Therefore, it is a challenge for any MAH to implement the regulations, and this is particularly true where a company's PV department or team is small (i.e., less than five).

"Outsource!" "Use a CRO!" "Use consultants or contractors!" I hear you cry, but outsourcing, consultants, or contractors can make life easier or more difficult depending on your perspective. Managing any resource, especially one that is not internal, means that you need to understand the work they are carrying out for you and the outputs to be delivered. This is key to them knowing if they are performing and delivering as needed because, regardless of whether your PV team is internal, external, or a mixture of the two, you still have to meet the MAH obligations. Broadly speaking, PV can be split into a few areas:



- Day-to-day case processing: here, the focus is on the individual report and compliance with regulatory reporting requirements. It is, by nature, reactionary – we react to the reports received
- Aggregate reports and signal detection: here, the focus is on looking at combined or aggregate data for particular products – either cumulatively or for a specific time period. This is proactive and involves detailed planning and organisation

- Training: here, the focus is that not only is appropriate training delivered to all staff at the MAH, but that staff involved in PV are suitably trained and continue their professional development
- PV management and oversight: here, the focus is more on how processes are carried out, how systems are working, and whether everything is in place. This is a combination of reactive and proactive processes

A review of any of the GVPs gives lists of tasks or processes that need to be carried out by any PV team. The next step is to take that list and look at what resources are required for the team to fulfil.

Taking one task or process as an example (such as aggregate reports or case processing), we can start to break down the larger tasks into smaller sub-tasks and then look at the resources needed to fulfil them.

As you can see from Table 1, training and/or accreditation for any task is an integral part of all processes, just as it is with GCP. In PV, our professional development is covered in GVP I, which states that all personnel involved in the performance of PV activities shall receive initial and continued training. For MAHs, this training relates to the roles and responsibilities of the personnel. Therefore, we need to be clever with how we balance budgetary needs against legal and staff needs for training. Companies are now moving away from face-to-face and off-site training because of the costs involved in taking staff away from their job for periods of time and are looking more at web-based or online solutions to meet training needs. Whatever solution is the best fit where you work, it has to, above all else, deliver the right level of training to the right audience. It would be of little value to deliver training on case processing and how to enter a case onto a safety database if you work in accounts. However, to someone in this role, it is invaluable.

Task	Case processing	Aggregate reports
Sub-tasks	• Triage • Data entry • Quality control checks • Medical review • Submissions • Identification and request follow-up information	• Writing • Literature searching • Interpretation of data • Medical review
Resources	• Processes to follow? • Training/ accreditation to undertake? • Expertise in all sub-tasks? • Database for processing?	• Processes to follow? • Expertise? • Training/ accreditation to undertake? • Templates to follow? • How do I get listings and tabulations? • Where do I get sales data from? • Where do I get product information from?

Table 1: Case processing and aggregate reports

No system is perfect, no system will get it right every time, and all systems can improve. The role of audits and inspections in PV is to help identify areas for improvement. Be that small or large, it is these improvements in any system that help us learn and grow professionally.

Integrating GDPR into PV Processes

Understanding whether you, or your organisation, processes personal data is critical to understanding whether the EU GDPR applies to your activities (5).

Personal data in PV are seen early on in the process chain during day-to-day case processing. This is because, in PV, one of the requirements for an adverse event case report to be considered a valid individual case safety report is the existence of an identifiable patient (6). Once it is possible to identify an individual directly or indirectly from the information you are processing, that information may be considered personal data (7). Having a subject/patient/consumer's name or initials (with or without a combination of other information such as date of birth), ID number, or even IP address along with one or more other factors (such as those specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person) could result in the identification of an individual.

In fact, for PV, there is no running away from GDPR, and it is not something to be taken lightly, with breaches facing fines of up to €20 million or 4% of annual global revenue, whichever is highest.

The regulation, which came into force on 25 May 2018, has been the most important change in data privacy in 20 years and is based on seven key principles, which can be found in Article 5 of the GDPR (2016/679).

Under GDPR, data subjects have a set of rights that they can evoke against companies or organisations that process their personal data (8).

It is important that companies or organisations have at least a basic interpretation of the principles, rights, and requirements of GDPR in company policies and guidance documents

that employees can follow when implementing the requirements within their processes. There are points to consider under each key principle.

First, personal data should be processed lawfully, fairly, and in a transparent manner. Do you have explicit consent from the data subject for use of their personal data? Data subjects must give their consent freely and subjects must be informed transparently on how their data will be used and protected. Data subjects must be provided with the option to opt out if they wish to. Also, you should review how the consent is sought and make a record of it.

As a point of note, health data (together with other sensitive data) are subject to a general prohibition on processing without informed consent, unless an exception applies. An exception to the health data prohibition on processing (without informed consent) is provided in Article 9(2)(i), which recognises that processing of data is necessary to fulfil PV legislation.

Is the processing compliant with a legal obligation? In the interest of public health, MAHs have PV obligations to receive, process, and report adverse event data to a competent authority, and to safeguard patients. This also includes maintaining the confidentiality of subject's data.

Are the personal data being held and processed fairly with consideration of the subject's rights? You should ensure that subjects are made aware of the processing of their personal data, what safeguarding is in place, and how they can exercise their rights in relation to the processing of their personal data.

Can you disclose to the subject clearly and thoroughly the personal data you hold about them upon their request? Under GDPR, subjects have the right to request the personal data concerning them. These data must be presented in a readable format or that which can be easily transmitted and accessed by the subject (data portability).

The second principle is that data collected from the subject for specified, explicit, and legitimate purposes should not be further processed. Data must only be collected and processed for the sole purpose of which the data are being collected, based on a legal obligation (in this case, PV legislation).

Third, the personal data collected should be adequate, relevant, and limited to what is necessary for the purposes of collection/processing. Only the information required for that intended purpose must be collected, processed, and stored. The data must be adequate enough for the intended purpose. The data should be limited or not exceed what is required. Also, access to the data within the organisation must be limited to relevant personnel


Image: © Pixabay

and companies, ensuring appropriate back-up procedures are in place to prevent data losses.

Fourth, the personal data collected and processed should be accurate and, where necessary, rectified or erased. Are the personal data you hold on your system up to date? You should ensure that a review of the data is carried out regularly, as required, to maintain its accuracy. The data must be up to date and remain current.

Fifth, the personal data should be kept no longer than is necessary for the purposes for which the personal data are processed. Do you have a retention schedule for personal data storage? Do you have appropriate measures in place to safeguard the subjects' data rights? You should ensure the data are stored for the defined periods as described in your company's retention schedule, with adequate safeguard measures in place to ensure integrity is maintained and that the data subjects' rights are not compromised. For electronic data, consider password protection. For hard copies, keep data in locked cupboards with access limited only to the relevant personnel. Where third parties are used for data archiving, details should be clearly documented in a contractual agreement. There must be arrangements defined for who, within the company, would have access to the archive data.

Sixth, the personal data should be secured in an appropriate manner. Are the personal data subject to access by unauthorised people? Are they secure from accidental loss, destruction, or damage? Consider the use of confidential waste bins, shredders, and have a clear desk policy. Desktops and laptops must be screen locked when left unattended. If data are transferred to other countries, ensure there are provisions for data protection in that country. If it is necessary to transfer data, have contractual agreements in place.

Do you have back-up processes and a business continuity plan in place for uncertainties? Your company's business continuity plan must work for your PV function. The use of a database to store subject data can mitigate any data loss, damage, and destruction. Also, appropriate safeguard measures must be put in place to ensure regular back-ups of the system.

Finally, the controller should be responsible for demonstrating compliance with the regulation. As a data controller, can you demonstrate that your processes are robust for handling personal data under the GDPR requirements? To be accountable, you must fully understand the legal obligations of PV, the key GDPR principles, and the rights of data subjects. Once this is clearly understood, you can ensure that adequate processes and measures are in place to remain compliant with GDPR at all times.

In PV, we have a legal obligation to collect health data to fulfil the purposes of public safety (9). Your privacy notice should include your lawful basis for processing data, as well as the purposes of this processing. A data privacy notice must be clear and easily understood. This will help you comply with your accountability obligations under the GDPR. Data protection legislation is there to ensure people can trust you to use and store their data fairly and responsibly for legitimate purposes.

References

1. Visit: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:348:0074:0099:EN:PDF
2. Visit: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:348:0001:0016:EN:PDF
3. Visit: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0352&from=EN
4. Visit: www.ema.europa.eu/en/human-regulatory/post-authorisation/pharmacovigilance/good-pharmacovigilance-practices
5. Visit: www.eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
6. Visit: www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-good-pharmacovigilance-practices-gvp-module-vi-collection-management-submission-reports_en.pdf
7. Visit: www.ico.org.uk/for-organisations/data-protection-act-2018
8. Visit: gdpr-info.eu
9. Visit: www.pipaonline.org/write/MediaManager/Members%20Area/Pharmacovigilance/Interim_guidance_notes_on_UK_data_protection_in_post-marketing_pharmacovigilance.pdf

About the authors

Emma Boulton is the Head of Pharmacovigilance for UK and Ireland at Napp Pharmaceuticals. She has over 20 years of PV experience in both pre- and post-marketing. Emma is a serving committee member of PIPA and the Co-Chair of the PIPA training working party. Emma is a qualified nurse and holds a post-graduate diploma in Pharmacovigilance.

Dora Amene is the Pharmacovigilance Manager at TMC Pharma Services. She is a serving committee member of PIPA and Co-Editor for PIPA's journal, which is published at least three times a year. Dora has a Master's degree in Pharmacovigilance and seven years of PV experience in post-marketing and, recently, in clinical.