Dr Lincoln Tsang Partner
lincoln.tsang@apks.com
Arnold & Porter Kaye Scholer LLP, London

The continued legislative and policy development of the EudraVigilance database

EudraVigilance is a huge database containing over 10 million separate data entries. It was first launched in 2001 to manage and analyse information in the form of individual case safety reports ('ICSRs') on suspected adverse reactions to medicines. The system is hosted by the European Medicines Agency ('EMA') which operates the system on behalf of the medicines regulatory network of the Member States of the EU and EEA. EudraVigilance has evolved over the years in order to respond to the ever changing environment in which medicines are being developed, prescribed, used, monitored and regulated, including most recently in the shape of a new version of the system that is due to go live on 22 November 2017. Dr Lincoln Tsang, Partner at Arnold & Porter Kaye Scholer LLP, here explores the purpose and development of the EudraVigilance system, looks at the new, updated system, and considers the impact of Brexit on the UK's involvement in drug safety regulation and access to the EudraVigilance system going forward.

Historical development

The EU Regulation governing the centralised procedure contemplates that the database must be accessible to the general public, updated and managed independently of pharmaceutical companies. The Regulation moreover states that EudraVigilance must facilitate the search for specific prescribing and use information for authorised medicines such as package leaflets and summaries of product characteristics, and information on medicines that are authorised for use with children. The publicly accessible information must be worded in language that is comprehensible to lay people.

In 2010, the EMA's management board adopted a EudraVigilance Access Policy, which came into force in July 2011 and outlined the data elements for and instructions on how to access ICSRs from EudraVigilance for drug regulators, health professionals, patients and consumers, marketing authorisation holders in the EU/EEA and research organisations.

Most recently, the management board of the EMA endorsed the launch on 22 November 2017 of an improved EudraVigilance system for collecting and monitoring suspected adverse events. This was announced by the EMA on 22 May 2017.

Architecture and functionalities of EudraVigilance

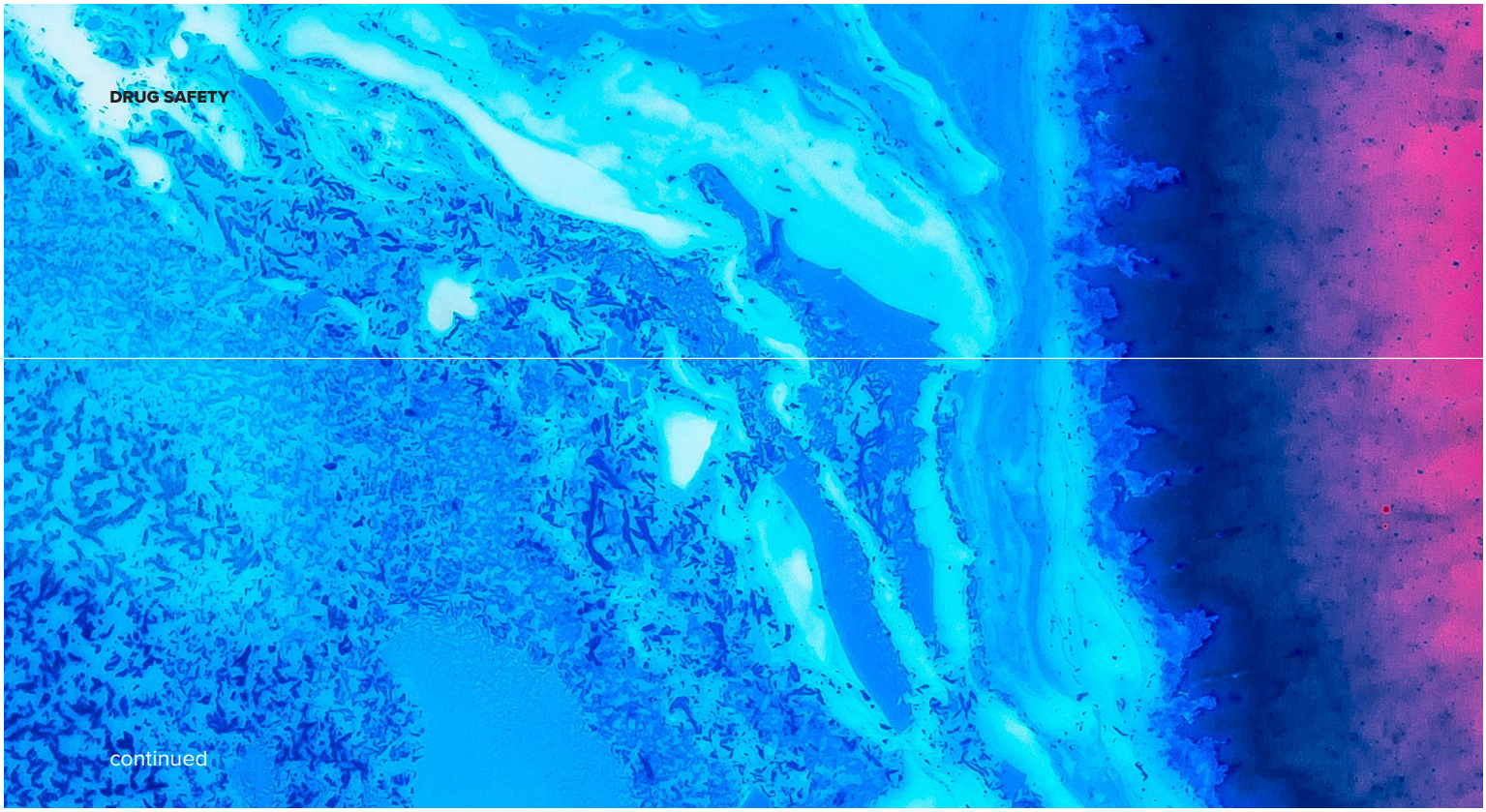
Having a large database is necessary for the purpose of conducting drug safety monitoring in order to detect new safety signals especially those that occur less frequently but are serious and that may impact the safe and effective conditions of a medicine. Since EU regulators are able to access the database, new methods, such as the proportional reporting ratio, can be developed to mine data for new signals. In addition, preliminary results may enable regulators including PRAC to assess new safety signals earlier with a view to considering appropriate measures to mitigate the attendant risks associated with the use of a medicine.

EudraVigilance supports the efforts of ensuring safe and effective use of medicines authorised in the EU/EEA in a manner that facilitates:

- electronic exchange of ICSRs among the EMA, national competent authorities, marketing authorisation holders and sponsors of clinical trials in the EU/EEA;
- early detection and evaluation of possible safety signals; and
- better product information for medicines authorised in the EU/EEA.

Operationally, the EMA and national competent authorities of the EU/EEA are responsible for regularly reviewing and analysing EudraVigilance data to detect safety signals. The Pharmacovigilance Risk Assessment Committee ('PRAC'), a pan-European specialist advisory committee for drug safety established under the new pharmacovigilance legislation in 2010, evaluates the safety signals detected in EudraVigilance and may recommend regulatory action as a result. For example, in 2016, following a detailed examination of the emerging safety information, the EMA, following consultation with PRAC, issued the following important new safety measures:

- New contraindication for riociguat (which is a stimulator of soluble guanylate cyclase) in patients with symptomatic pulmonary hypertension associated with idiopathic interstitial pneumonia or PH-IIP;
- Product information to be updated



continued

to strengthen existing warnings for posaconazole (an antifungal agent) that the two dose forms given by mouth cannot be simply interchanged as this may lead to underdosing and to a potential lack of efficacy;
- New recommendations to minimise the risk of diabetic ketoacidosis in patients taking SGLT2 inhibitors which are used for treating Type 2 diabetes;
- New recommendations to minimise the risk of progressive multifocal leukoencephalopathy (a rare brain infection) in patients taking natalizumab, a biological product indicated for treating multiple sclerosis;
- Updated recommendations for use of idelialisib (which is a phosphoiosidtide 3-kinase inhibitor indicated for treating certain haematological malignancies) to minimise the risk of serious infections in cancer patients treated with this medicine;
- Use of metformin to treat diabetes expanded to patients with moderately-reduced kidney function based an assessment of glomerular filtration rate with revision of contradiction and information on doses, monitoring and precautions in patients with reduced kidney function; and
- Updated prescribing information on potential risk of toe amputation for SGLT2 inhibitors authorised for the treatment of diabetes.

Electronic reporting is now mandatory for marketing authorisation holders and sponsors of clinical trials. The architecture of EudraVigilance is designed to support electronic transmission ICSRs between electronic data interchange partners, namely the EU regulatory authorities, the marketing authorisation holders and sponsors of clinical trials. Specifically, EudraVigilance is underpinned by two functional components: (a) a fully automated safety and message processing mechanism using XML based messaging; and (b) a large pharmacovigilance database with query and tracking functions.

Before an organisation can provide electronic submission within the EudraVigilance production environment, it is necessary to perform testing. Testing is necessary to ensure that the local safety or pharmacovigilance database is compatible with the EudraVigilance system and compliant with messaging format and terminology requirements. Testing applies to organisations that electronically report ICSRs to EudraVigilance for the first time or organisations that introduce a major change to their local safety/pharmacovigilance database that might impact electronic reporting. The EMA enables all the electronic data interchange partners to register and connect to the test environment to analyse and test whether their software/IT system is interoperable with EudraVigilance. The EudraVigilance test encompasses six distinct steps, namely:

- Register with EudraVigilance;
- Confirmation to use the EudraVigilance gateway;
- A communication test to assure successful gateway-to-gateway communication;
- Development and validation testing for data exchange between the EMA and the marketing authorisation holder or sponsor;
- XML test phase for organisations using the internationally accepted format for ICSRs; and
- Production to commence electronic transmission of ICSRs.

Certain aspects of drug safety reporting have already been the subject of the international harmonisation process under the auspices of the International Council on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use sponsored by the United States, the EU and Japan. Accordingly, EudraVigilance complies with the formats and standards for collection, collation and reporting safety information.

Public access to EudraVigilance

In the era of greater transparency in regulatory decision making, the EMA has developed a policy governing the level of access to the data held in EudraVigilance by different stakeholder groups. The stakeholders are divided into six groups to determine the level of data access, and there are six levels of data access. For example, EU/EEA medicines regulatory authorities can access at Level 3 all ICSRs without restrictions to carry out their public obligations on pharmacovigilance. Similarly, marketing authorisation holders have Level 3 access to all ICSR data elements without restrictions for them to fulfil their pharmacovigilance

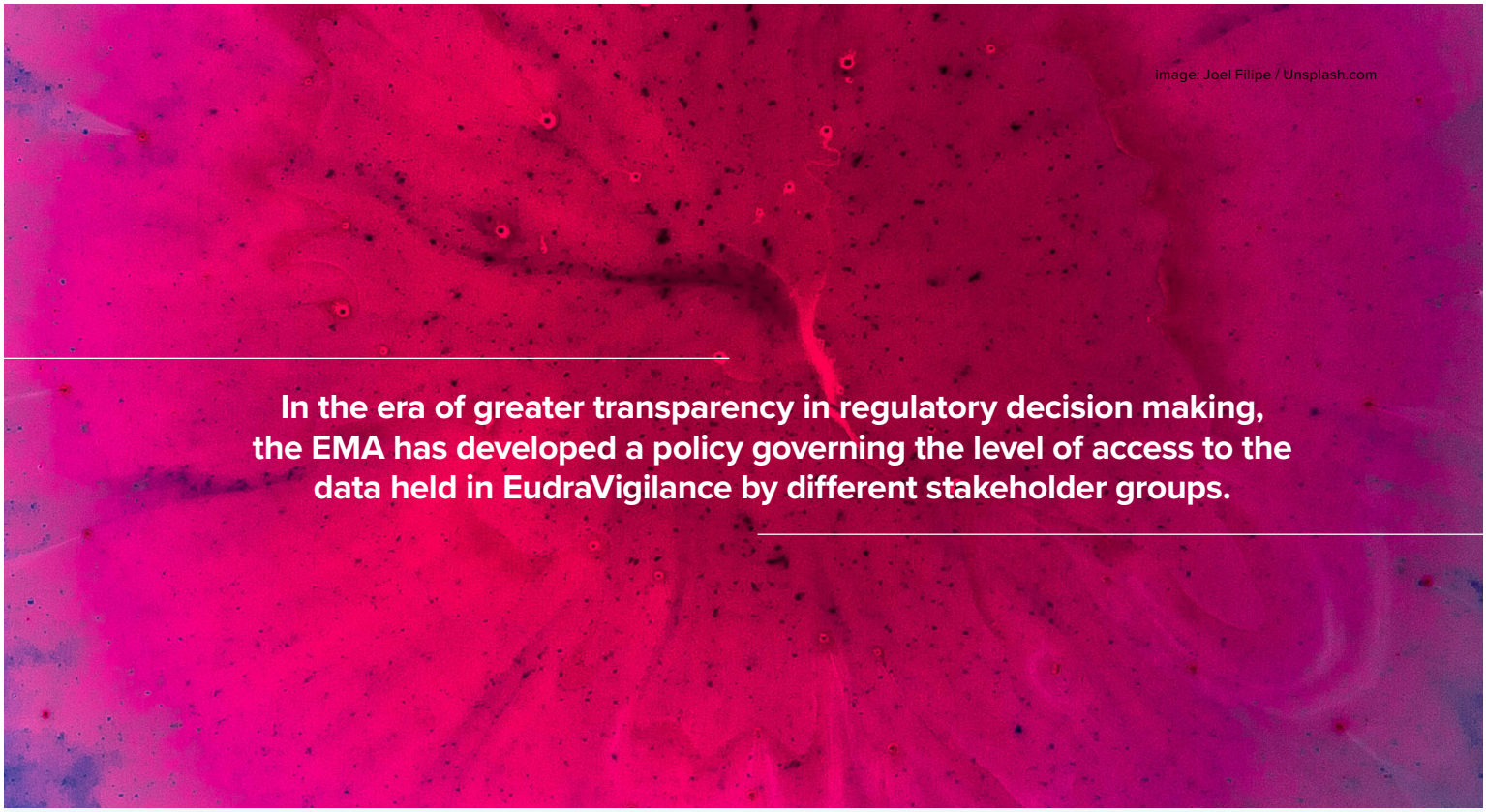


image: Joel Filipe / Unsplash.com

In the era of greater transparency in regulatory decision making, the EMA has developed a policy governing the level of access to the data held in EudraVigilance by different stakeholder groups.

obligations, based on the ICSRs reported by the holders and those resulting from the medical literature monitoring activities performed by the EMA.

The policy for public access was first adopted in December 2010 by the EMA Management Board and came into force in July 2011. The policy describes the guiding principles relating to access to ICSRs contained in EudraVigilance by medicines regulatory authorities, marketing authorisation holders in the EU/EEA, healthcare professionals, patients and consumers as well as academia who all have a vested interest in drug safety. Moreover, under the new policy, in view of increasingly globalised efforts in drug safety monitoring, the World Health Organisation ('WHO') as well as medicines regulatory authorities outside of the EEA are now permitted to access the database at Level 2C. That means that these regulatory bodies outside the EU/EEA can access an extended subset of ICSR data elements to enable them to carry out their respective responsibility to protect public health outside of the EU/EEA and, in the case of WHO, globally.

Granting of broader data access is provided through progressive changes to the EU legislative framework following adoption of the new pharmacovigilance legislation in 2010 whilst maintaining compliance with rules to protect personal data to take account of the 2009 Opinion of the European Data Protection Supervisor. The Opinion states, amongst other things, that the overall operation of the pharmacovigilance system relies on the processing of personal data. These data are included in the reporting of adverse drug reactions and can be considered as personal because they reveal information about drug use and associated health problems. Processing of such data is, in the Data Protection Supervisor's view, subject to strict EU data protection rules.

The extent of data access has been the subject of an administrative complaint to the European Ombudsman by a journalist working with the *New York Times* in the case 1252/2014. The complaint is concerned with the refusal by the EMA to grant the complainant public access to EudraVigilance. The EMA informed the complainant that it had already made public much of the requested information. It refused to give him access to any information that had not already been made public. The complainant requested that the EMA provide reasons for its refusal. The EMA confirmed that further public access would be contrary to the rules on the protection of personal data and privacy.

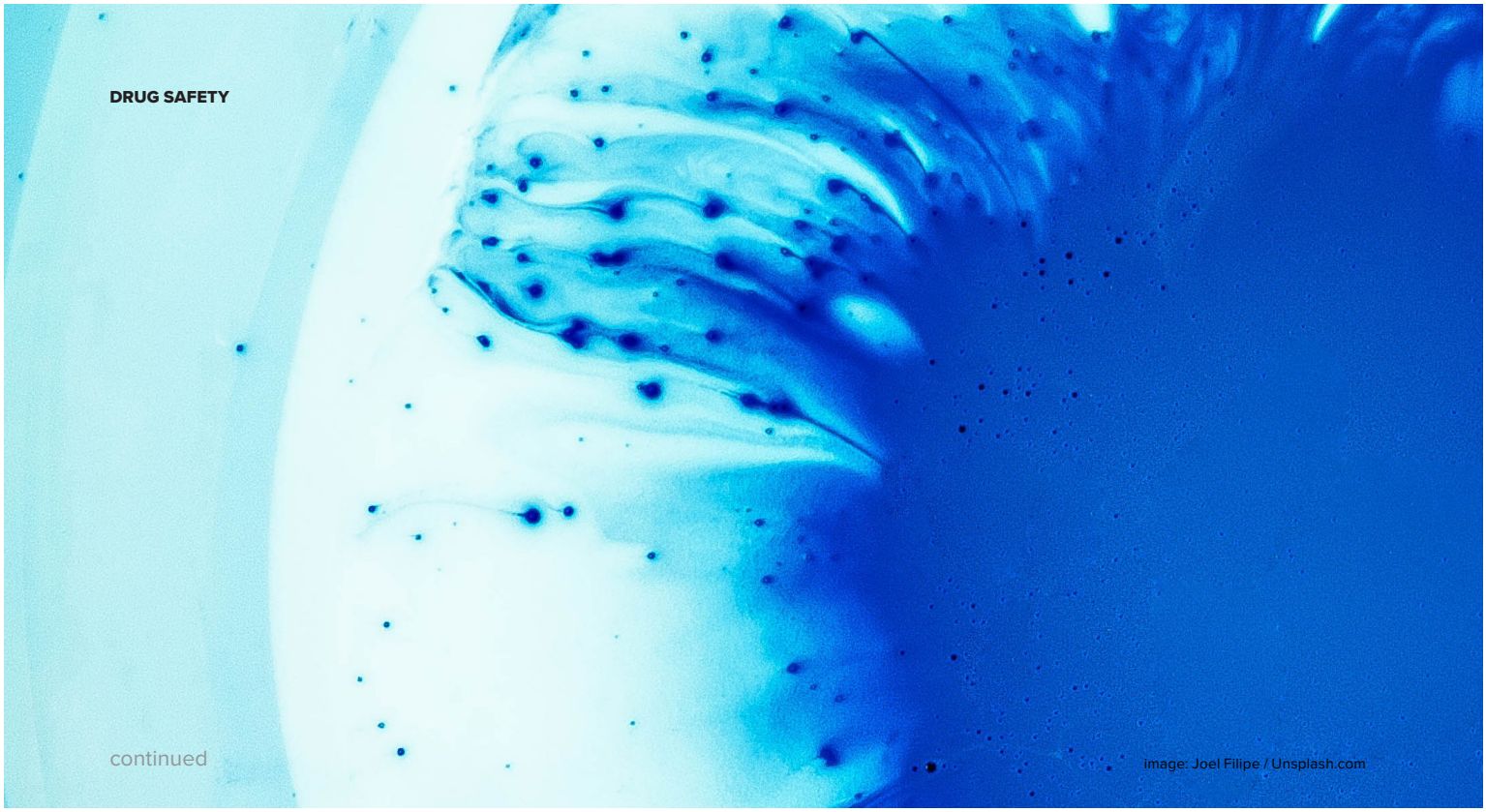
The complaint turned on the journalist's right to gain access to an entire database in the public interest for him to carry out 'ground-breaking' work based on an analysis of the data to identify possible patterns in the safety data. He argued that privacy could be safeguarded by not giving access to any data field containing sensitive information. Specifically, in the case, the journalist sought to gain access to non-aggregated safety data whereas the EMA makes publicly available aggregated data from EudraVigilance.

The Ombudsman noted the extreme sensitivity of non-aggregated data in EudraVigilance. If any personal data in the ICSRs were disclosed, either directly or indirectly, this would give rise to a very serious breach of the privacy of the patients. In the ruling, the Ombudsman considered that whilst an individual report is assigned a code number which can be redacted to ensure that the data cannot be linked directly back to the data subject. However, even if this were done, it might not be sufficient to ensure that the data in EudraVigilance is effectively anonymised thanks to technological advances in 'data crunching.' The Ombudsman noted at paragraph 24:

"Advances in computing power and the availability of huge amounts of data on the internet regarding individuals (such as data on social media platforms) may now make it technically possible, at least for some persons or companies with access to these technical means, to link what appears to be anonymised data from EudraVigilance to at least some identifiable persons."

Following the investigation, the Ombudsman ruled in favour of the EMA and found no instances of maladministration.

In conjunction with the public access policy, in April 2017, the EMA adopted a best practice guide for management of authorised access to EudraVigilance,



continued

image: Joel Filipe / Unsplash.com

reflecting the EMA's commitment to confidentiality, integrity and availability of its information systems and the safety of its assets. The purpose of the best practice guide is to ensure information security when using EudraVigilance, especially protection of the confidentiality of ICSRs and the rights of the data subjects in compliance with the data protection and privacy rules.

The new EudraVigilance system

Following an independent audit and a favourable recommendation from PRAC, the EMA's Management Board confirmed in May 2017 that the new version of EudraVigilance is fully functional and ready to go live on 22 November 2017.

In the lead up to the launch of the new EudraVigilance system, the EMA advises that national competent authorities, marketing authorisation holders and sponsors of clinical trials have to make final preparations to ensure that their processes and IT infrastructures can work with the new system. Specifically, organisations that have already established electronic submission of ICSRs to EudraVigilance should perform the gateway configuration and communication testing with XCOMP in advance of the launch of the new version of the EudraVigilance on 22 November 2017. Testing will require organisations to use the specific format of ICSRs for electronic transmissions to ensure compatibility for file uploading and conversion. Consistent with the legislative aim of the pharmacovigilance legislation and the policy of better regulation, the new EudraVigilance system supports enhancement and improves efficiency of safety monitoring.

The new functionalities introduced into the new version of EudraVigilance sought to address the following five principal considerations:

- Enhancement of signal detection and data analysis tools to support safety monitoring by regulatory authorities and marketing authorisation holders;
- Improvement in quality, completeness and searchability of ICSRs to facilitate data analysis;
- Enhancement of the scalability of the EudraVigilance system;
- Simplification of reporting of ICSRs to EudraVigilance to obviate the need to report the same data to individual national regulatory authorities in the EU/EEA by virtue of the re-routing function; and
- Enhanced capability for all ICSRs for suspected adverse reactions in the EU/EEA to be made available to the WHO Uppsala Monitoring Centre in recognition of the need for closer global cooperation between the EU/the EEA and the WHO.

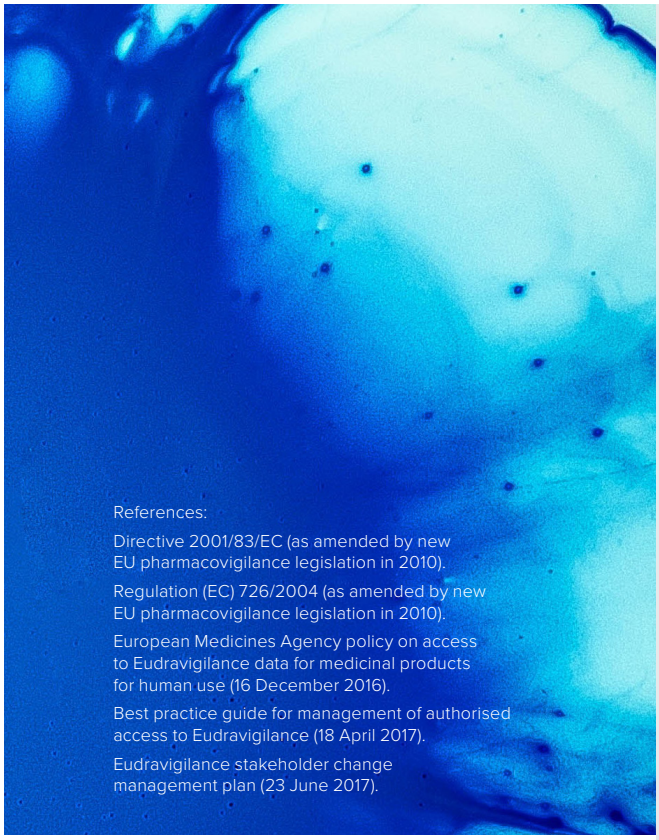
In preparation for the new system, the EMA has indicated that it will support national competent authorities, the marketing authorisation holders and sponsors of clinical trials in the EU/EEA through targeted e-learning and face-to-face trainings, webinars and information days. Users have been able to trial the new functions of the EudraVigilance system and the internationally agreed format for ICSRs in a test environment as of 26 June 2017.

The reporting of adverse reactions by patients and healthcare professionals to national competent authorities based on local spontaneous reporting systems will remain unchanged. There will also be no changes to the reporting of suspected unexpected serious adverse reactions during clinical trials until the application of the new Clinical Trial Regulation.

The impact of Brexit

The UK has been a key contributor in shaping legislative and policy developments within the EU/EEA and globally especially in relation to drug safety. EudraVigilance bears some close resemblance to the national Adverse Drug Reaction Online Information Tracking system, which was the brainchild of the UK regulatory agency.

The adopted guidelines of the European Council of Ministers as well as the European Commission implementing documents have made it clear that after 29 June 2019, the UK will become a 'third country' and will no longer be a Member State of the EU. The new relationship will be the subject of negotiations after the terms of exiting the EU are agreed and settled within a very ambitious timetable. The European Commission and the UK contemplate in their joint statement that the negotiations themselves will last approximately 18 months starting from early June 2017 to October/November 2018.



References:

Directive 2001/83/EC (as amended by new EU pharmacovigilance legislation in 2010).

Regulation (EC) 726/2004 (as amended by new EU pharmacovigilance legislation in 2010).

European Medicines Agency policy on access to Eudravigilance data for medicinal products for human use (16 December 2016).

Best practice guide for management of authorised access to Eudravigilance (18 April 2017).

Eudravigilance stakeholder change management plan (23 June 2017).

Certainty and long term stability as well as the sustainability of the sector will become critically important in the challenging time ahead. The ability for the UK to continue making its contribution to EU medicines regulation is plainly important for the sake of business continuity but also in the interest of patient safety and public health. Moreover, it should be recognised that drug safety is a global public health imperative which does not recognise geographical boundaries and that regional and international cooperation is critically important.

To avoid the 'cliff edge' effect of Brexit, on 5 July 2017, the Secretaries for Health and Business of the UK Government expressed their desire in an open letter in the *Financial Times* to continue to collaborate with the EU based on three principles:

1. patients should not be disadvantaged;
2. innovators should be able to get their products into the UK market as quickly and simply as possible and
3. the UK continues to play a leading role promoting public health.

It remains unclear whether the UK, as a 'third country' outside of the EU, will enjoy the same level of access to the EudraVigilance system to protect UK citizens and on what terms. It should be recognised that setting up a national pharmacovigilance database system can be costly and will have implications for resources, particularly in the current climate of austerity.

Government accepts Caldicott and CQC recommendations

The UK Government published its response to the recommendations made by the National Data Guardian, Dame Fiona Caldicott ('NDG'), and the Care Quality Commission ('CQC') on 12 July 2017, in relation to the data security, opt-out and consent policies for health data within the UK's health and social care system. The response document, 'Your Data: Better Security, Better Choice, Better Care,' sets out the UK Government's intention to uphold all the recommendations made by the NDG in the 'Review of data security, consent and opt-outs' and by the CQC in its 'Safe data, safe care: data security' review.

The NDG's review criticised the NHS' current data security, recommending that the NHS' Information Governance Toolkit be updated and that it integrates the NDG's set of ten 'data security standards.' These standards include access being restricted to 'personal confidential data' to all but those who need it only for as long as they need it, identifying and responding to cyber attacks as soon as possible with the advice of CareCERT, making breach reports within 12 hours of detection, and holding IT suppliers accountable via contracts for protecting the personal confidential data they process. "The standards recommended by the NDG seem robust," said Valerie Surgenor, Partner at MacRoberts, who adds however that they "seem very ambitious to implement and continually monitor. For example 'standard 3' says that all staff should complete annual training and pass a mandatory test - what would happen if a large number of staff failed this?"

The UK Government states that 'a framework will be in place to support organisations to move to the latest operating system by March 2018,' in response to the CQC noting that the NHS' use of outdated, unsupported systems poses data security vulnerabilities. The CQC further commented that human activity, such as working around system rules in an insecure way in order to improve efficiency, was also a major cause of data insecurity. The CQC recommended that, in addition to redesigning IT systems and data protocols around the needs of patient care, 'all staff should be provided with the right information, tools, training and support to allow them to do their jobs effectively while still being able to meet their responsibilities for handling and sharing data safely.'

The Government has announced an initial £21 million increase to the £50 million investment in data and cyber security already being provided to the NHS, to increase the cyber resilience of major trauma sites as an immediate priority, and to improve NHS Digital's national monitoring and response capabilities.

The NDG also made recommendations relating to consent, transparency regarding the use of citizens' health data, and the use of opt-out models. The Government has agreed *inter alia* to implement a revised consent/opt-out model 'to allow people to opt out of their personal confidential data being used for purposes beyond their direct care' and to roll out an online service for citizens to 'see more clearly how their data collected by NHS Digital has been used for purposes other than their direct care' by March 2020. "The new system points towards a more 'user preference' type of data management for data subjects, which seems positive," said Surgenor. "Education will be key to ensuring patients understand."