EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Considerations on the international transfer of personal (health) data in ICSRs originating in the EU

Training Module EV-M8

Content summary

- EudraVigilance: the different stakeholders, their applicable data protection frameworks and accountability
- Core principles of the EU General Data Protection Regulation (GDPR) and the importance of data pseudonymisation
- Reporting of adverse drug reactions: interplay between pharmacovigilance legislation and the EU GDPR
- International transfer of personal (health) data originating in the EU
- Transfer tools for the international transfer of personal (health) data originating in the EU
- Where to seek data protection advice?
- Sources of information

EudraVigilance (EV)

Different stakeholders involved in the processing of health-related information in EV:

- National Competent Authorities (NCAs) in the EEA, European Commission (EC), EMA;
- Marketing authorisation holders (MAHs);
- Sponsors of Clinical Trials;
- Patients, healthcare professionals, academia, public.

Applicable data protection framework:

- Regulation (EU) 2016/679 – EU General Data Protection Regulation (GDPR): applicable to MAHs & Sponsors;
- Regulation (EU) 2018/1725 – EU Data Protection Regulation (EU DPR): applicable to EU Institutions.

Accountability:

- Joint controllers of EudraVigilance system: EC, EMA, NCAs;
- Controllers in their own rights: MAHs & Sponsors.

Regulation (EU) 2016/679 – the GDPR

The General Data Protection Regulation (GDPR) applies since 25 May 2018. It sets out detailed requirements for organisations collecting, storing and managing personal data.

When does the GDPR apply?

The GDPR applies if a company:

- processes **personal data** and **is based in the EU**, regardless of where the actual data processing takes place;
- is **established outside the EU but** offers goods or services to individuals in the EU, or monitors the behaviour of individuals within the EU, thereby **processing their personal data**.

Non-EU based businesses processing EU citizen's data have to appoint a **representative in the EU**.

When does the GDPR not apply?

The GDPR does **not** apply if:

- the data subject is a legal person (i.e., an organisation);
- the processing is done by a person acting for purposes which are outside his trade, business, or profession;
- the data subject is deceased; however national laws may apply.

Regulation (EU) 2016/679 – the GDPR

Article 4(1) of the GDPR defines **Personal data** as:

- Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or (…) factors specific to the physical, physiological, genetic (…) identity of that person;

Article 4(5) of the GDPR defines **Pseudonymisation** as:

- the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Regulation (EU) 2016/679 – the GDPR

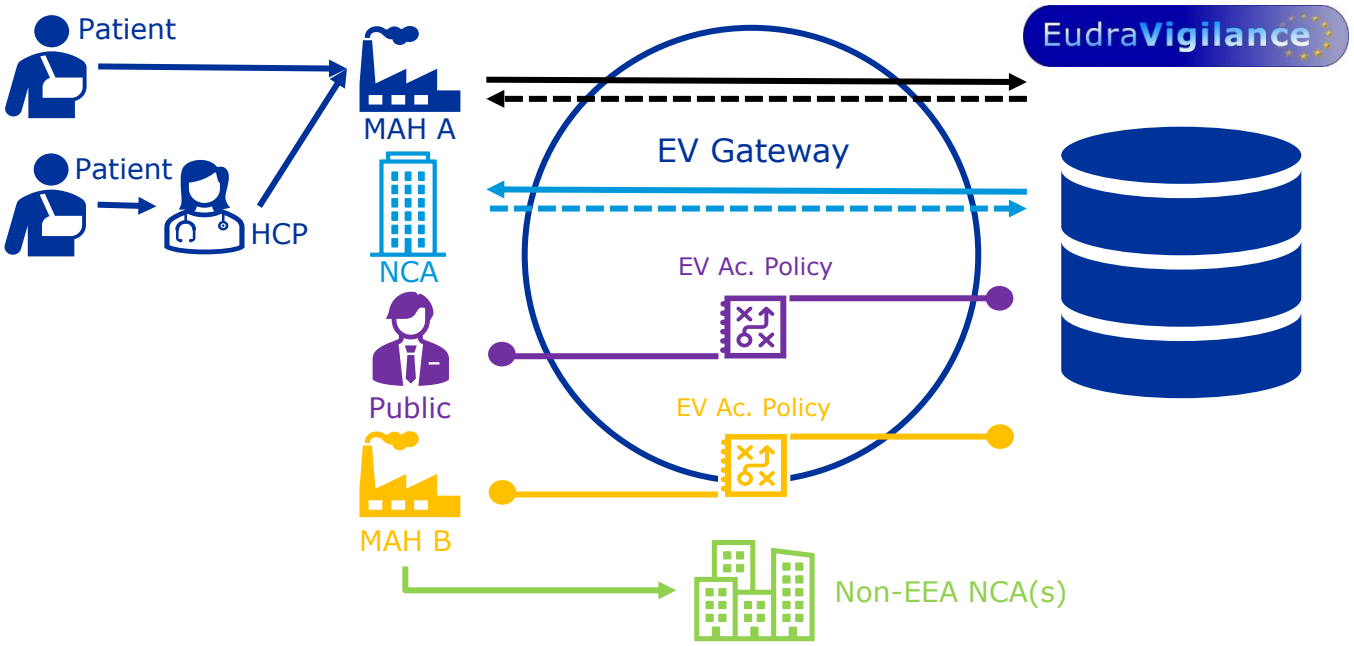
Article 4(15) of the GDPR defines **Data concerning health** as:

- 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;

Article 4(15) of the GDPR states that **Personal Data concerning health**:

- should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services (…); a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

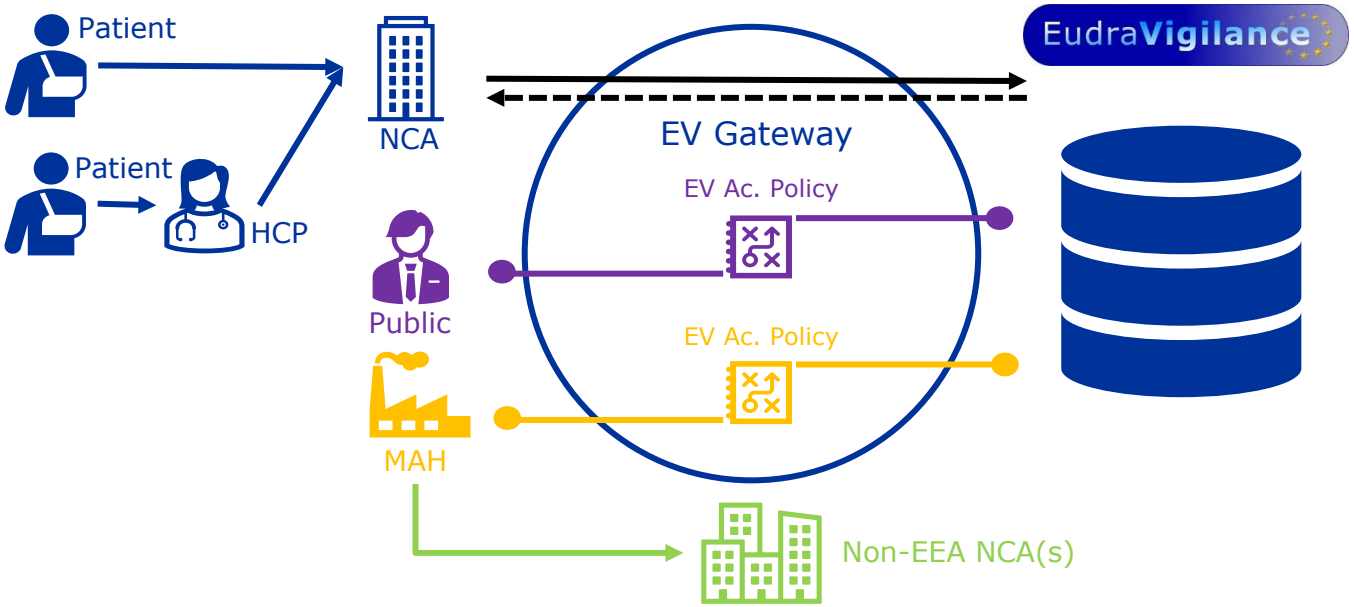
Most common ways for information exchange amongst multiple stakeholders in the EU/EEA - **MAHs**



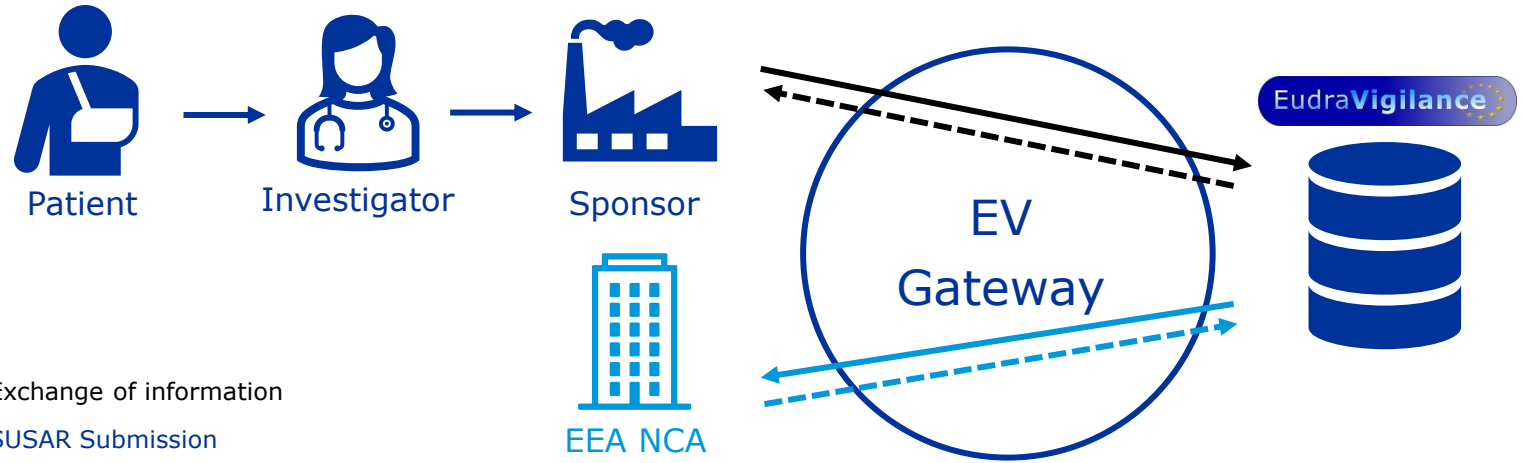
Key

- Exchange of information
- ICSR Submission
- ACK message
- Rerouted ICSR (if requested by NCA)
- ACK message
- Public access to the EV database via the ADRReports.eu portal (access **only** for Spontaneous PM reports, in accordance with the EMA's EV Access Policy)
- ICSR Download by MAH (access in accordance with the EMA's EV Access Policy)
- ICSR Submission by EEA MAH B to Non-EEA NCA(s) - if applicable

Most common ways for information exchange amongst multiple stakeholders in the EU/EEA - **MAHs**



Most common way for information exchange amongst multiple stakeholders - **Sponsors**



Key

- Exchange of information
- SUSAR Submission
- ACK message
- Rerouted SUSAR (if requested by NCA)
- ACK message

Why is pseudonymisation important?

Fully identifiable personal data

Maximum utility
Maximum risk

Pseudonymised data

Reduced utility
Reduced risk

Anonymised data

Minimum utility
Minimum risk

Significant **risks** to the protection of data subjects.

- Potential risks may impact the **interests** and **rights of the data subject.**
- They could lead, inter alia, to **discriminatory effects on natural persons** on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, etc.

The application of **pseudonymisation** to personal data can **reduce the risks to data subjects**.

- It also helps controllers and processors to meet their data protection obligations;
- As the data utilisation is greater than the one obtained via an anonymisation technique, better decisions can be taken.

For data to be rendered truly anonymous, an anonymisation technique must be **irreversible**.

- However, as a result, **the utility of the data may be impaired, depending on the purpose for which it is used for**.

Example of pseudonymised data sent to EV - **MAHs**

Fully identifiable personal data

Name/Initials: John Smith
DOB/Age: 23.SEP.1986
Gender: Male
Email: john.smith@email.com

Pseudonymised data

Name/Initials: ***MSK*** **nullflavor**
DOB/Age: 23.SEP.1986
Gender: Male

Notes:

- This example does **not** to intend to provide official guidance regarding data protection, namely on what actions may or may not need to be taken by MAHs when dealing with ICSRs, regardless of their provenance (for example, a case directly communicated to the company by the Reporter or a report obtained by the MAH from EudraVigilance, via L2A download).
- The pseudonymised data shown above is a simple representation of what the fictitious data could look like when sending the report to EV, based on the personal data received by the MAH in the ADR report of the dummy patient.
- As the Sender of the case received the information directly from the Primary Source and has the source documentation, the data in EV is considered pseudonymised and thus not as anonymised given that, ultimately, the Sender can establish a link between the case and the patient.

Example of pseudonymised data sent to EV - **Sponsors**

Fully identifiable personal data

Name/Initials: John Smith
DOB/Age: 23.SEP.1986
Gender: Male
Investigation number: AC-129-09

Pseudonymised data

Name/Initials: ***MSK*** **nullflavor**
DOB/Age: 23.SEP.1986
Gender: Male
Investigation number: AC-129-09

Notes:

- This example does **not** to intend to provide official guidance regarding data protection, namely on what actions may or may not need to be taken by Sponsors when dealing with SUSARs.
- The pseudonymised data shown above is a simple representation of what the fictitious data could look like upon sending the report to EV, based on the information received by the Sponsor in the SUSAR report of the dummy patient sent by the Investigator.
- As the Sender of the case received the information directly from the Primary Source and has the source documentation, the data in EV is considered pseudonymised and thus not as anonymised given that, ultimately, the Sender can establish a link between the case and the patient.

Reporting of adverse drug reactions

Legal Requirements/Pharmacovigilance legislation

When an organisation receives a report directly from a Reporter (for MAHs and NCAs) or from the Investigator (for Sponsors), it has to process data to meet the reporting requirements in line with local and, if applicable, international requirements.

In the EU, the requirements for the reporting of suspected adverse reactions (ICSRs and SUSARs) to EudraVigilance are set out in:

- **Sponsors:** Regulation (EU) No 536/2014; the **format** and **content** of ICSRs is further defined by the Commission Implementing Regulation (EU) No 520/2012;
- **MAHs:** Regulation (EC) No 726/2004 and Directive 2001/83/EC; the **format** and **content** of ICSRs is further defined by the Commission Implementing Regulation (EU) No 520/2012 and the applicable Good Pharmacovigilance Practices (GVPs), namely GVP Module VI.

Reporting of adverse drug reactions

Application of the GDPR

In line with the provisions of the GDPR, **MAHs** and **Sponsors are data controllers** for the personal data processing activities carried out pursuant to the **clinical trials and pharmacovigilane (PhV) legislation**, including the access and **further processing** of ICSR data originating in from EudraVigilance.

- **A data controller** is a legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- "**Further processing**" **includes** access and **onward transfers** of ICSRs originating in the EU, independently of the origin (for example, a report from a Consumer/Investigator or case received from another sender), mode of access granted (for MAHs: EV, EVDAS) and level of access granted (e.g. granularity of the fields).

Reporting of adverse drug reactions

Application of the GDPR

PhV/Safety systems need to ensure compliance with the provisions set out in the GDPR.

- Those adaptations are subject to the **MAH's** and **Sponsor's own data protection assessment** regarding the risks to the rights and freedoms of natural persons;
- This includes the implementation of the **necessary technical and organisational measures,** for example:
  - protecting access to the systems with passwords
  - granting access rights to the PhV database only to certain authorized users and reviewing access rights at regular intervals
  - ensuring that, by default, only personal data which are necessary for fulfilling each specific legal requirement are processed

Reporting of adverse drug reactions

Application of the GDPR

In order to comply with their data protection obligations, organisations may pseudonymise personal data before sending reports to EV (for example, they can replace the patient's name or initials or the date of birth with the "MSK" nullflavor in the ICSR reports).

However, the pseudonymisation should **NOT** obstruct the fulfilment of their PhV obligations.

Organisations must adhere to the content and format of the reports as defined in EU legislation!

Reporting of adverse drug reactions

Note on the use of nullflavors

NullFlavors are a collection of codes specifying why a valid value is not present in an ICSR.

They are available with the ICH-E2B(R3) format and refer to instances where a value is :

- Not known by the sender
  - For example, the age of the patient is unknown: code "**UNK**";
- Available to the sender of the ICSR but it is **masked** because the sender chooses not to provide it due to data protection reasons.
  - For example, the date of birth of the patient cannot be shared due to local data protection laws: code "**MSK**".

Reporting of adverse drug reactions

Note on the use of nullflavors

As per the EU Individual Case Safety Report (ICSR) Implementation Guide, certain data elements foresee the use of the nullflavor "**MSK**". This indicates to the receiver of an ICSR that the (initial) sender of the ICSR holds the information but is/was **unable to send this information due to data protection reasons**.

It is acknowledged that for *certain* data elements that can identify an individual such as the Patient (name or initials) (*ICH E2B(R3) D.1*) or the Date of Birth (*ICH E2B(R3) D.2.1*), the "**MSK**" flag *can* be appropriate.

However, the use of the "**MSK**" nullflavor in an ICSR should be made in accordance with national and/or European data protection laws. In other words, the "**MSK**" nullflavor should **NOT** be routinely used by companies - **it should be reserved ONLY for cases where data genuinely needs to be redacted to comply with data protection legislation.**

Access to data in EudraVigilance - **MAHs**

Article 24(2) of Regulation (EC) 726/2004 defines several level of access to EV:

- EV is fully accessible to the NCAs of the Member States and to EMA and the EC;
- EV is accessible to MAHs to the extent necessary for them to comply with their **PhV obligations**.

The EV Access Policy implements the varying access levels by determining which stakeholder groups have access to each data field.

As already explained in S11 of this training course, MAHs (Stakeholder group III) have access to:

- L1 ICSRs (Public subset of ICSR data elements)
- **L2A ICSRs (to fulfil their PhV obligations)**
- **L2B ICSRs (for signal evaluation and other PV activities – see slide 20)**
- L3 ICSRs (MAH's own cases and MLM cases)

International transfer of personal (health) data originating in the EU - **MAHs**

Considering that EEA-based MAHs may have:

1) Affiliates/subsidiaries in third countries who are required to comply with local PhV legislation; and/or
2) Licensing partners in third countries with whom ICSR data may be required to be exchanged (if there is a Safety Data Exchange Agreement (SDEA) in place between the parties)

This may require the MAH to report ICSRs that contain **personal health data** to a country outside the EU.

This transfer of data may qualify as an **international transfer of personal (health) data**. The GDPR provides for mechanisms to do so which are further explained by the EDPB: International data transfers | European Data Protection Board.

International transfer of personal (health) data originating in the EU - **MAHs**

L2A ICSR download: MAHs should note that if they are required to share ICSR data originating from EV, they are requested to **only** use the reports obtained via **L2A download**.

L2B ICSR download: Considering the provisions of Annex C of the EV Access Policy, L2B ICSR Downloads requests by MAHs are **only** applicable:

- Following the initial signal management steps as outlined in the GVP Module IX have been performed, including a reference to the corresponding e-RMR if applicable;
- Given a review of ICSR data in the context of a pharmacovigilance assessment procedure such as the PSUR as outlined in GVP Module VII or when required by the PRAC in a referral or signal assessment procedure;

International transfer of personal (health) data originating in the EU - **Sponsors**

Considering that Sponsors often run Clinical Trials in multiple countries, including in non-EEA countries, health data originating in the EU may have to be sent to outside the EU.

This transfer of data may qualify as an **international transfer of personal (health) data**.

The GDPR provides for mechanisms to do so which are further explained by the EDPB: International data transfers | European Data Protection Board.

International transfer of personal (health) data originating in the EU

Despite of these transfer requirements that EEA-based organisations may have, the GDPR imposes **limitations** on transfer of personal data outside the EEA:

- **The level of protection of individuals granted by the GDPR should remain essentially equivalent**, despite the transfer of health-information to third countries;
- Personal data may only be transferred outside of the EEA in compliance with the conditions laid down in **Chapter V of the GDPR**, for example, the organization shall:
  - Have an appropriate **legal basis** for transferring personal data to a third country;
  - Rely an appropriate **transfer tool** (as provided by articles 45 and 46 of the GDPR) - see EDPB guidance International data transfers | European Data Protection Board; and
  - Only transfer the personal data that are necessary to achieve the purpose of the transfer (**data minimization principle**).

International transfer of personal (health) data originating in the EU

MAHs and **Sponsors** are **accountable** for complying with the rules set out in Union data protection legislation when transfer personal data i.e., the GDPR and national data protection laws where applicable.

MAHs and Sponsors shall adhere to the rules applicable to the transfer of personal data to third countries as set out in Chapter V of the GDPR and the confidentiality undertaking of the EudraVigilance Access Policy (the last one is only applicable for MAHs).

International transfer of personal (health) data originating in the EU

Transfer tools

Article 45 of the GDPR – Transfers on the basis of an adequacy decision

The European Commission has the power to determine (Article 45 of the GDPR) whether a country outside the EU (i.e. third country) offers an adequate level of data protection by adopting an adequacy decision.

The effect of such an adequacy further safeguard being necessary. The list of countries which are currently recognized by the EC as providing an adequate level of data protection is available at:

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

International transfer of personal (health) data originating in the EU

Transfer tools

Article 46 of the GDPR – Transfers subject to appropriate safeguards

In the absence of a decision pursuant to Article 45 of the GDPR, an organization may transfer personal data to a third country or an international organisation only if it has provided **appropriate safeguards**, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Article 46 lists the transfer tools which may provide appropriate safeguards.

In the absence of adequacy decision and before transferring ICSRs containing personal data to third countries, MAHs and Sponsors rely on an **appropriate transfer tool**.

Where to seek data protection advice?

In case of question relation to personal data protection, **MAHs/Sponsors should first seek advice from their Data Protection Officer** and then, if needed, **from their data protection authority (DPA)**.

The competent data protection authority is the authority in the EU Member State where the company is based. The list of DPAs is available at:

https://edpb.europa.eu/about-edpb/about-edpb/members_en

If the MAH/Sponsor processes personal data in or across several EU member states or is part of a group of companies established in several EU member states, the competent DPA may be located in another EU Member State than the one in which the MAH/Sponsor is established.

Sources of information

Regulation (EU) 2016/679 (EU GDPR): https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2018/1725 (EU DPR): https://eur-lex.europa.eu/eli/reg/2018/1725/oj

Regulation (EU) No 536/2014: https://eur-lex.europa.eu/eli/reg/2014/536/oj

Commission Implementing Regulation (EU) No 520/2012: https://eur-lex.europa.eu/eli/reg_impl/2012/520/oj

Regulation (EC) No 726/2004: https://eur-lex.europa.eu/eli/reg/2004/726/oj

Directive 2001/83/EC: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001L0083

Commission Implementing Regulation (EU) No 520/2012: https://eur-lex.europa.eu/eli/reg_impl/2012/520/oj

GVPs: https://www.ema.europa.eu/en/human-regulatory-overview/post-authorisation/pharmacovigilance-post-authorisation/good-pharmacovigilance-practices-gvp

GVP VI (EMA/873138/2011): https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-good-pharmacovigilance-practices-gvp-module-vi-collection-management-and-submission-reports-suspected-adverse-reactions-medicinal-products-rev-2_en.pdf

Sources of information

EMA EV Access Policy (EMA/759287/2009): https://www.ema.europa.eu/en/documents/other/european-medicines-agency-policy-access-eudravigilance-data-medicinal-products-human-use-revision-4_en.pdf

EMA EV Access Policy - Confidentiality undertaking for MAHs (EMA/337295/2016): https://www.ema.europa.eu/system/files/documents/other/wc500206426_en.pdf

International data transfers (European Data Protection Board): https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en

Adequacy decisions (European Commission): https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Data Protection Authorities in the EU: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

Summary of EV-M8

We are now at the end of the training Module EV-M8, which provided you the basis for understanding:

- EudraVigilance: the different stakeholders, their applicable data protection frameworks and accountability
- Core principles of the EU General Data Protection Regulation (GDPR) and the importance of data pseudonymisation
- Reporting of adverse drug reactions: interplay between pharmacovigilance legislation and the EU GDPR
- International transfer of personal (health) data originating in the EU
- Transfer tools for the international transfer of personal (health) data originating in the EU
- Where to seek data protection advice?
- Sources of information