



London, 29 October 2004  
Doc. Ref: EMEA/115735/2004

## EUDRAVIGILANCE TELEMATICS IMPLEMENTATION GROUP

### NOTE FOR GUIDANCE ON THE ELECTRONIC DATA INTERCHANGE (EDI) OF INDIVIDUAL CASE SAFETY REPORTS (ICSRs)<sup>1</sup> AND MEDICINAL PRODUCT REPORTS (MPRS) IN PHARMACOVIGILANCE DURING THE PRE-AND POST-AUTHORISATION PHASE IN THE EUROPEAN ECONOMIC AREA (EEA)

|   |  |
|---|--|
| <b>DISCUSSION AT THE EUDRAVIGILANCE TELEMATICS IMPLEMENTATION GROUP (TIG)</b> | May 2001, June 2001, March 2002, May 2002, September 2002, December 2002, June 2003, February 2004, May 2004 |
| <b>DISCUSSION AT THE EUDRAVIGILANCE TASK FORCE</b>                            | December 2003, February 2004, March 2004, July 2004  |
| <b>EUROPEAN PHARMACEUTICAL INDUSTRY CONSULTATION</b>                          | January 2003, July 2003, March 2004, September 2004  |
| <b>ADOPTED BY THE EUDRAVIGILANCE TIG</b>                                      | September 2004   |
| <b>DATE FOR COMING INTO OPERATION</b>   | November 2004  |

<sup>1</sup> ICSRs refer to the adverse reaction reporting as required by Regulation (EC) No. 726/2004, Directive 2004/27/EC and Volume 9 of the 'Rules Governing Medicinal Products in the European Union' and to the reporting of suspected unexpected serious adverse reactions (SUSARs) as required by Directive 2001/20/EC.

## **I. Objective and Scope**

This Note for Guidance describes the procedures on the Electronic Data Interchange (EDI) of Individual Case Safety Reports (ICSRs) and Medicinal Product Reports (MPRs) in pharmacovigilance in the pre- and post-authorisation phase and the roles of all involved stakeholders in the EEA i.e. the Competent Authorities (CAs), the Marketing Authorisation Holders (MAHs), Applicants and Sponsors of clinical trials.

The operational requirements and agreed standards for EDI and the secure exchange of Safety and Acknowledgement Messages as well as Medicinal Product Report Messages are outlined.

Further, this Note for Guidance specifies the technical requirements and the process of transmission of electronic reports and messages through the EudraVigilance Gateway established at the EMEA and describes the obligations that EDI partners have to adhere to in this process to assure a successful electronic communication.

The implications of electronic reporting with regard to the legal reporting compliance as defined in Community legislation, the evaluation steps and the recovery procedures in the event of a communication failure are also described.

The concepts of this Note for Guidance are also going to apply for the EDI processes of any other pharmacovigilance data, which are currently still under development (e.g. PSUR data).

## II. Definitions

The definitions that are described in this chapter are the general definitions used throughout this Note for Guidance and are aimed to ensuring an unambiguous understanding of these terms.

Selected terminology as defined in the frame of the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use has been included with particular emphasis on the type of format (XML, SGML), information (reports) and messages (safety and acknowledgment messages) used in the EDI process in the area of pharmacovigilance in the pre- and post-authorisation phase. As there are different types of acknowledgement of receipt of an EDI message, it is clearly indicated which level of acknowledgement is referred to, in order to avoid confusion.

For the purpose of this Note for Guidance, the following terms are defined as:

### II.1. EDI:

Electronic Data Interchange is the electronic transfer, from computer to computer, of commercial and administrative data using an agreed standard to structure an EDI message. EDI is based on the use of structured and coded messages, the main characteristic of which is their ability to be processed by computers and transmitted automatically and without ambiguity. This makes EDI specific in comparison with other data exchange such as electronic mail.

### II.2. EDI Message:

An EDI Message consists of a set of segments, structured using an agreed standard, prepared in a computer readable format and capable of being automatically and unambiguously processed.

### II.3. Gateway:

A Gateway is defined as a data exchange service, which consists of all core standards and functionality required for supporting the standards of the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) (e.g. Simple Mail Transfer Protocol/Secure Multipurpose Internet Mail Extension - SMTP/SMIME- protocol).

### II.4. Message Disposition Notification (MDN):

The MDN is a notification on the receipt of an EDI Message returned by the Receiver's Gateway to the Sender's Gateway. The MDN concludes a Message Transaction performed between two parties in a Gateway to Gateway communication.

### II.5. EDI Partner:

An organisation exchanging EDI Messages in the area of pharmacovigilance in the pre- and post-authorisation phase with another organisation. For the purpose of this Note for Guidance EDI partners in the pre- and post-authorisation phase in pharmacovigilance are as follows:

- Competent Authorities in the EEA
- Marketing Authorisation Holders in the EEA
- Applicants
- Sponsors in the EEA

### II.6. Sender:

The Sender is the person or entity creating an EDI Message for transmission.

### II.7. Receiver:

The Receiver is the intended recipient of the EDI Message.

## II.8 Report Sender:

The Report Sender is the person or entity creating a Safety Message as EDI Message in order to submit a Safety Report, which for the purpose of this Note for Guidance is an EDI Partner. In the Report Transaction the Report Sender will always remain the same, whereas with the exchange of messages the “Sender” and “Receiver” roles will change (see graph in Annex I). The same concepts apply to the organisation creating a Medicinal Product Message as EDI Message in order to submit a Medicinal Product Report, which for the purpose of this Note for Guidance is an EDI Partner being an Applicant, a Marketing Authorisation Holder or a Sponsor (see graph in Annex II).

## II.9. Report Receiver:

The Receiver is the intended recipient of the transmission of a Safety Message, which for the purpose of this Note for Guidance is an EDI Partner. The Receiver is also the intended recipient of the transmission of a Medicinal Product Report Message, which for the purpose of this Note for Guidance is an EDI Partner being the EMEA.

## II.10. Sender Identifier (Sender ID):

The Sender Identifier is the identification (ID) or combined EDI qualifier and ID of the Sender.

## II.11. Receiver Identifier (Receiver ID):

The Receiver Identifier is the identification or combined EDI qualifier and ID of the recipient.

## II.12. Message Transaction:

A Message Transaction is a set of actions encompassing the electronic transmission of an EDI Message (Safety Message, Acknowledgement Message, Medicinal Product Message) between a Sender and a Receiver including the return of the Message Disposition Notification for that message.

## II.13. Safety Message:

A Safety Message is an EDI Message including the information provided for one/more Individual Case Safety Reports contained in one Safety File exchanged between one Sender and one Receiver in one Message Transaction.

## II.14. Medicinal Product Report Message (MPRM):

A Medicinal Product Report Message is an EDI Message including the information provided for one/more Medicinal Product Reports contained in one Medicinal Product File exchanged between one Sender and one Receiver in one Message Transaction.

## II.15. Safety File:

The Safety File is the electronic file transmitted in one Message Transaction between one Sender and one Receiver containing one Safety Message.

## II.16. Medicinal Product File:

The Medicinal Product File is the electronic file transmitted in one Message Transaction between one Sender and one Receiver containing one Medicinal Product Report Message.

## II.17. Individual Case:

An Individual Case is the information provided by a primary source to describe suspected adverse reaction(s)/suspected unexpected serious adverse reactions related to the administration of one or more medicinal products/investigational medicinal products to an individual patient at a particular point of time.

## II.18. Individual Case Safety Report (ICSR):

An Individual Case Safety Report is a document providing the most complete information related to an Individual Case at a certain point of time. An ICSR may also be referred to as Safety Report.

II.18. Medicinal Product Report (MPR):

A Medicinal Product Report (MPR) is an electronic report with a defined set of data elements to populate and update the EudraVigilance Medicinal Product Dictionary (EVMPD). A Medicinal Product Report may contain information on an authorised Medicinal Product/ Investigational Medicinal Product.

II.19. Acknowledgement of Receipt:

The Acknowledgement of Receipt is the procedure by which on receipt of the Safety Message/Medicinal Product Report Message the syntax and semantics are checked.

II.20. Acknowledgement Message (ICSRACK):

The Acknowledgement Message is an EDI Message with the information on the result of the Acknowledgement of Receipt procedure to acknowledge the receipt of one Safety Message and the Safety Report(s) contained in the Safety File.

II.21. Acknowledgement Message (MPRACK):

The Acknowledgement Message is an EDI Message with the information on the result of the Acknowledgement of Receipt procedure to acknowledge the receipt of one Medicinal Product Report Message and the Medicinal Product Report(s) contained in the Medicinal Product File.

II.22. Report Transaction:

A Report Transaction is the complete set of actions in the electronic reporting of Safety Messages to comply with regulatory requirements which routinely includes the following:

- Creation of a Safety Message;
- Transmission of the Safety Message to the Report Receiver;
- On receipt of the Safety Message by the Receiver's Gateway return of an MDN;
- This MDN will be referred to as ICSR-MDN;
- The ICSR-MDN is received and stored by the Report Sender to document the success of the Safety Message transmission;
- The Safety Message is subjected to the Acknowledgement of Receipt procedure by the Report Receiver;
- The Acknowledgement Message is created;
- The Acknowledgement Message is returned to the Report Sender (technically the Report Receiver is a Message Sender for this part of the transaction);
- On receipt of the Acknowledgement Message by the Report Sender's Gateway return of an MDN;
- This MDN is referred to as ICSRACK-MDN;
- The ICSRACK-MDN is received and stored by the Report Receiver to document the successful transmission of the Acknowledgement Message;
- The Acknowledgement Message is evaluated to document the success of the Report Transaction.

II.23. Medicinal Product Report Transaction:

A Medicinal Product Report Transaction is the complete set of actions in the electronic reporting of Medicinal Product Messages, which routinely includes the following:

- Creation of a Medicinal Product Report Message;
- Transmission of the Medicinal Product Report Message to the Report Receiver;
- On receipt of the Medicinal Product Report Message by the Receiver's Gateway return of an MDN;
- This MDN will be referred to as MPR-MDN;
- The MPR-MDN is received and stored by the Report Sender to document the success of the Medicinal Product Report Message transmission;
- The Medicinal Product Report Message is subjected to the Acknowledgement of Receipt procedure by the Report Receiver;
- The Acknowledgement Message is created;

- The Acknowledgement Message is returned to the Report Sender (technically the Report Receiver is a Message Sender for this part of the transaction);
- On receipt of the Acknowledgement Message by the Report Sender's Gateway return of an MDN;
- This MDN is referred to as MPRACK-MDN;
- The MPRACK-MDN is received and stored by the Report Receiver to document the successful transmission of the Acknowledgement Message;
- The Acknowledgement Message is evaluated to document the success of the Report Transaction.

#### II.24. Competent Authorities:

- An authority within the EEA including the EMEA and the European Commission responsible for the granting of marketing authorisations for medicinal products and the supervision of marketing of such products in accordance with the relevant laws and regulations established under Community law.
- An authority within the EEA responsible for granting the authorisation to conduct a clinical trial in at least one Centre located with the Community in accordance with the relevant laws and regulations established under Community law.

#### II.25. Marketing Authorisation Holders:

All Marketing Authorisation Holders (MAHs) holding a valid marketing authorisation for a medicinal product in the EEA including any part thereof, independent of the authorisation procedure of this medicinal product.

#### II.26. Applicant:

An applicant is a pharmaceutical company applying for a marketing authorisation in the EEA.

#### II.27. Sponsor:

An individual, company, institution or organization, which takes responsibility for the initiation, management and/or financing of a clinical trial.

#### II.28. Investigational Medicinal Product (IMP):

An Investigational Medicinal Product is defined as a pharmaceutical form of an active substance or placebo being tested or used as a reference in a clinical trial, including products already with a marketing authorisation but used or assembled (formulated or packaged) in a way different from the authorised form, or when used for an unauthorised indication, or when used to gain further information about the authorised form.

#### II.29. Medicinal Product:

A Medicinal Product is defined as

- Any substance or combination of substances presented as having properties for treating or preventing disease in human beings; or
- Any substance or combination of substances, which may be used in or administered to human beings either with a view to restoring, correcting or modifying physiological functions by exerting a pharmacological, immunological or metabolic action, or to making a medical diagnosis.

#### II.30. Standard Generalized Markup Language (SGML):

The Standard Generalized Markup Language (SGML) is an International Standard (ISO 8879) computer language for describing a document in terms of its content (text, image) and logical structure (chapters, paragraphs, etc.) It is a standard for how to specify a document markup language or tag set. Such a specification is itself a document type definition (DTD). SGML is not in itself a document language, but a description of how to specify one. It is a metalanguage. SGML is based on the idea that documents have structural and other semantic elements that can be described without reference to how such elements should be displayed.

II.31. XML:

Extensible Markup Language (XML) is a subset of SGML that is completely compatible with SGML.

II.32. The EudraVigilance Gateway:

The EudraVigilance Gateway is the data-processing network as defined in the Community legislation and is providing a single point of contact between MAHs, Applicants, Sponsors and Competent Authorities in the EEA. By doing so, the EudraVigilance Gateway is considered a hub and all connections to the EDI Partners are known as spokes. Safety, Acknowledgement and Medicinal Product Report Messages are routed through the hub to the desired spoke.

II.33. The EudraVigilance Database Management System (DBMS):

The EudraVigilance Database Management System (DBMS) is the pharmacovigilance database defined in Community legislation.

### **III. Processing and Acknowledgement of Receipt of Safety Messages and Medicinal Product Report Messages**

#### **III.1. Processing and Acknowledgement of Receipt of Safety Messages**

The process flow is described in the flowchart in Annex 1, which should be read in association with this chapter.

For routine electronic reporting a Safety Message including one or several ICSRs is sent by the Report Sender in internationally (ICH) agreed electronic format through an electronic Gateway to the Report Receiver, which for the purpose of this guideline is an EDI Partner as defined in chapter II. The electronic Gateway of the Report Sender encrypts the message and dispatches it through the Internet. The Report Receiver's Gateway automatically returns a MDN upon receipt of the message, decrypts the message and forwards it to the Report Receiver's locally established pharmacovigilance system. In the following this MDN will be referred to as ICSR-MDN.

In the Report Receiver's locally established pharmacovigilance system the arriving Safety Message is processed following the Acknowledgement of Receipt procedure and a corresponding Acknowledgement Message (ICSRACK) is returned by the Report Receiver to the Report Sender. The ICSRACK will be transmitted from the Report Receiver's Gateway to the Report Sender's Gateway, which thereupon automatically returns a MDN upon receipt of the Acknowledgement Message. In the following this MDN will be referred to as ICSRACK-MDN.

A Safety Message is successfully recognised and validated when:

- a) The Sender and the Receiver could be correctly identified in the Safety Message i.e. both the Sender and the Receiver must be a registered EDI Partner of the EudraVigilance Gateway,
- b) The Safety Message is well-formed i.e. a valid XML file,
- c) The Safety Message is in accordance with the ICH ICSR Document Type Definition (DTD) in the latest version as adopted at Community level (Annex 4) i.e. the message instances, which define each element of the ICSR being transmitted and reflect how the various data elements are related to each other, are correct,
- d) The Safety Message and the Safety Reports are in full compliance with the business rules adopted at Community level (Annex 4).

The EudraVigilance Gateway will reject Safety Messages automatically, if they are not in accordance with point a), b) and c). As a result, it is the sole responsibility of the Sender to ensure that the above criteria are fully met so that the Safety Message can be recognised successfully by the EudraVigilance Gateway.

A Safety Message is successfully transmitted, when the Report Sender receives an ICSR-MDN. The date of the ICSR-MDN will serve as the official receipt date of the transmission of the Safety Message by the EudraVigilance Gateway and documents the fulfilment of the reporting timelines as defined in Community legislation.



The successful transmission, though fulfilling the requirements of receipt of an ICSR-MDN, does not indicate acceptance of the Safety Message by the Receiver's locally established pharmacovigilance system in the Acknowledgement of Receipt procedure.

In this procedure the Receiver verifies the semantics, syntax, format and content both on the message and the report level. The Acknowledgment Message, as defined in the frame of the ICH E2B(M) and M2 Expert Working Group is generated which indicates acceptance or rejection. A rejection in the Acknowledgement of Receipt procedure resulting in an acknowledgement code 02 or 03 does not constitute regulatory compliance.

The sender of a message that has been rejected by the EudraVigilance Gateway in part or in total has the obligation to resubmit corrected versions immediately within the reporting timelines as defined in Community legislation, so that the message can be accepted in the locally established pharmacovigilance system of the Receiver. In validated and tested systems and after passing a production pilot testing this case should be a rare exception.

The detailed steps in the Acknowledgement of Receipt procedure are as follows:

Following the successful receipt of the Safety Message, the Report Receiver is responsible for loading the ICSR(s) into the locally established pharmacovigilance system. Further, the Report Receiver is responsible for generating, at the latest within two business days, an Acknowledgement Message, providing the validation status of each ICSR, which is the subject of the Safety Message of the particular transmission.

The Acknowledgement Message can reflect three different types of transmission acknowledgements at Safety Message level:

- ACK code 01: All ICSRs loaded into the Report Receiver's locally established pharmacovigilance system;
- ACK code 02: ICSR error, not all ICSRs loaded into the Report Receiver's locally established pharmacovigilance system;
- ACK code 03: XML parsing error, no data extracted from the Safety Message

The Acknowledgement Message can reflect two different types of transmission acknowledgements at ICSR level:

- ICSR code 01: ICSR loaded successfully into the Report Receiver's locally established pharmacovigilance system;
- ICSR code 02: ICSR not loaded into the Report Receiver's locally established pharmacovigilance system.

An ICSR must be acknowledged by the Report Receiver with the ICSR acknowledgement code 01 when it is in full compliance with the ICH and Community guidance documents referred to in Annex 4. Thereupon it will be loaded into the Report Receiver's locally established pharmacovigilance system.

In case the validation status of one or more ICSRs within one Safety Message is assigned the ICSR acknowledgement code 02, resulting in the transmission acknowledgement ACK code 02 i.e. ICSR error, not all ICSRs loaded into the Report Receiver's locally established pharmacovigilance database, the Report Sender must retransmit, upon receipt of the Acknowledgement Message, immediately a corrected version of the affected ICSRs electronically, if the validation rules according to the technical documentation (referred to in Annex 4) are not met.

If, following the receipt of the Acknowledgement Message, the transmission acknowledgement code is 03 in accordance with the relevant ICH standards and Community guidance documents as referred to in Annex 4, the entire corrected Safety Message needs to be immediately retransmitted electronically. Safety Messages with the transmission acknowledgement code 03 are not regarded as valid for reporting compliance purposes.

The Acknowledgement Message is sent by the Report Receiver of a Safety Message to the Report Sender of the Safety Message. At the Gateway level, an ICSRACK-MDN will be returned to the Sender of the Acknowledgement Message.

The date of the ICSRACK-MDN will serve as the official receipt date of the transmission of the Acknowledgement Message by the EudraVigilance Gateway.

From a conceptual point of view the following principles apply:

- The Report Receiver of a Safety Message, that requires an acknowledgement, shall not act upon the content of the Safety Message until such an ICSRACK is sent by the Report Receiver and successfully received by the Report Sender. If a Safety Message is entirely rejected (transmission acknowledgement code 03) by the Report Receiver, the Report Receiver of the Safety Message shall not act upon the content of the Safety Message until a corrected version is received and successfully acknowledged with an acknowledgement code 01.
- If a Safety Message contains ICSR errors leading to a transmission acknowledgement code 02, the Report Receiver of the Safety Message shall not act upon the ICSRs with the ICSR acknowledgement code 02 of this Safety Message until a corrected version of the ICSR(s) with the ICSR acknowledgement code 02 is received and successfully acknowledged with an ICSR acknowledgement code 01.

However, if a rejected ICSR(s) within a Safety Message contains important safety information, which raises public health concerns, the Report Receiver in liaison with the Report Sender may act upon this ICSR(s).

The same requirements outlined above for the successful recognition of a Safety Message apply to the Acknowledgement Message. It is the sole responsibility of the Sender of the Acknowledgement Message to ensure that these criteria are met and that the Acknowledgement Message can be recognised and routed successfully by the EudraVigilance Gateway.

In summary, two different levels of acknowledgement are available.

One acknowledgment for the transmission of messages via the Gateway of the EDI partners, is the message disposition notification (MDN), which is automatically sent upon the receipt of an EDI Message being either a Safety or Acknowledgement Message at the level of the Receiver's Gateway without any content verification. This MDN is the proof to the Sender that a Safety Message was received successfully by the Receiver and serves as evidence for any reporting timeline compliance measures as defined in Community legislation, if the Safety Message was successfully validated and recognised in accordance with the ICH and Community guidance documents (Annex 4) i.e. transmission acknowledgement code 01 and ICSR acknowledgement code 01.

The second, acknowledgement, is the Acknowledgement Message, which summarises the outcome of the Safety Message and ICSR validation by the Report Receiver.

If for technical reasons the Report Receiver does not return an MDN (being either an ICSR-MDN or an ICSRACK-MDN), alternative reporting measures may need to be taken by the Report Sender to maintain the compliance to reporting timelines as defined in Community legislation (please refer to chapter IV).

### **III.2. Processing and Acknowledgement of Receipt of Medicinal Product Report Messages**

The process flow is described in the flowchart in Annex 2, which should be read in association with this chapter.

For routine electronic reporting a Medicinal Product Message including one or several Medicinal Product Reports is sent by the Report Sender in accordance with the agreed electronic format (Annex 4) through an electronic Gateway to the Report Receiver, which for the purpose of this guideline is the EMEA as EDI Partner. The electronic Gateway of the Report Sender encrypts the message and dispatches it through the Internet. The Report Receiver's Gateway (the EudraVigilance Gateway) automatically returns a Message Disposition Notification (MDN) upon receipt of the message, decrypts the message and forwards it to the Report Receiver's locally established pharmacovigilance system (EudraVigilance DBMS). In the following this MDN will be referred to as MPR-MDN.

In the EudraVigilance DBMS the arriving Medicinal Product Report Message is processed following the Acknowledgement of Receipt procedure and a corresponding Acknowledgement Message (MPR-ACK) is returned by the Report Receiver to the Report Sender. The MPR-ACK will be transmitted from the Report Receiver's Gateway (the EudraVigilance Gateway) to the Report Sender's Gateway, which thereupon automatically returns a MDN upon receipt of the Acknowledgement Message. In the following this MDN will be referred to as MPR-MDN.

A Medicinal Product Report Message is successfully recognised and validated when

- a) The Sender and the Receiver could be correctly identified in the Medicinal Product Report Message i.e. both the Sender and the Receiver must be a registered EDI Partner of the EudraVigilance Gateway,

- b) The Medicinal Product Report Message is well-formed i.e. a valid XML file,
- c) The Medicinal Product Report Message is in accordance with the Medicinal Product Report XML Schema in the latest version as referred to in Annex 4 i.e. the message instances, which define each element of the Medicinal Product Report being transmitted and reflect how the various data elements are related to each other, are correct.
- d) The Medicinal Product Report and Medicinal Product Report Message are in full compliance with the business rules as referred to in Annex 4.

The EudraVigilance Gateway will reject a Medicinal Product Report Message automatically, if it is not in accordance with point a), b) and c). It is the sole responsibility of the Sender to ensure that the above criteria are fully met in order that the Medicinal Product Report Message can be recognised successfully by the EudraVigilance Gateway.

A Medicinal Product Report Message is successfully transmitted, when the MDN is returned to the Report Sender. The date of the MDN will serve as the official receipt date of the transmission of the Medicinal Product Report Message by the EudraVigilance Gateway.

Following the successful receipt of the Medicinal Product Report Message, the Report Sender receives an MPR-MDN. The Report Receiver is responsible for loading the Medicinal Product Report(s) into the EudraVigilance DBMS/EudraVigilance Medicinal Product Dictionary (EVMPD). Further, the Report Receiver is responsible for generating within two business days an Acknowledgement Message, providing the validation status of each Medicinal Product Report, which is the subject of the Medicinal Product Report Message of the particular transmission.

## **IV. Responsibility in Case of Communication Failure**

### **IV.1. Mechanical, programme, electronic or communication failure at the Report Sender side**

#### **IV.1.1 Failure of Safety Message generation**

In case of any mechanical, programme, electronic or communication failure, which prevents an EDI Partner from physically generating a Safety Message to another EDI Partner, a paper report in an internationally acknowledged format (e.g. CIOMS 1) should be sent instead. The date of the Report Sender's record of sending the paper report will be sufficient to prove regulatory compliance in an inspection of the Report Sender. The paper report will not be processed within the EDI Partner's locally established pharmacovigilance system but only stored for compliance purposes. Therefore, once the mechanical, programme, electronic or communication failure has been restored by the Report Sender, the Report Sender will retransmit electronically the Safety Message(s) containing the same versions of the ICSRs in full compliance with the content and the format as specified by the documents listed in Annex 4 to the intended EDI Partner(s) for processing and uploading into the locally established pharmacovigilance system. In the electronically retransmitted ICSRs the ICH E2B(M) section A.1.11 'Other case identifiers in previous transmissions' must be completed with all the identifiers used on the paper report.

Upon receipt of the electronic version of the Safety Message the Report Receiver will return the corresponding ICSR MDN and Acknowledgement Message via the Report Receiver's Gateway.

This scenario also applies when a Safety Message can be physically generated and transmitted but the Safety Message is acknowledged with a transmission acknowledgement code 02 or 03 and the correction of the error is not feasible to meet the reporting compliance time frame as defined in Community legislation (e.g. error is caused by a software problem that needs more time to resolve). The Report Receiver's local administrator should be notified and paper report(s) in an internationally acknowledged format (e.g. CIOMS 1) should be transmitted. Electronic retransmission of the affected Safety Message(s) needs to occur after the correction of the problem. In the electronically retransmitted ICSRs the ICH E2B(M) section A.1.11 'Other case identifiers in previous transmissions' must be completed with all the identifiers used on the paper report.

The paper report(s) transmitted in an internationally acknowledged format (e.g. CIOMS 1) should be clearly marked with 'FAILURE OF ELECTRONIC SAFETY MESSAGE GENERATION AT SENDER'S SIDE'.

#### **IV.1.2 Failure of Medicinal Product Message generation**

In case of any mechanical, programme, electronic or communication failure, which prevents an EDI Partner from physically generating a Medicinal Product Report Message to the Report Receiver (EMEA), EVWEB or the EudraVigilance Access Simple Database (EVSDB) can be used by the Report Sender to create a Medicinal Product Report Message. Upon receipt of the electronic version of the Medicinal Product Report Message the Report Receiver will return the corresponding MPR-MDN and Acknowledgement Message via the Report Receiver's Gateway.

#### **IV.1.3 Failure of message transmission on the Gateway level**

In case of a prolonged communication failure on the Report Sender side for successfully generated Safety Message(s), these can be via physical media following the EWG M2 Recommendation to the ICH Steering Committee for the Electronic Standards for the Transfer of Regulatory Information (ESTRI) Physical Media - Recommendation 2.1 and 2.2. Before initiating this procedure the Report Receiver's local administrator should be contacted. The Acknowledgement Messages will be returned on physical media. Since no ICSR-MDN will be generated in this process, the date of the Report Sender's record of sending the paper report will be sufficient to prove regulatory compliance in an inspection of the Report Sender.

### **IV.2. Mechanical or communication failure at the EudraVigilance Gateway and/or Database Management System (DBMS) at the level of the EMEA**

#### **IV.2.1 Failure of message receipt on the Gateway level**

In the event of a prolonged non-availability of the EudraVigilance Gateway, as confirmed by the EMEA, the Report Sender should send the

- Safety Messages to the Report Receiver(s) via physical media following the EWG M2 Recommendation to the ICH Steering Committee for the Electronic Standards for the Transfer of Regulatory Information (ESTRI) Physical Media - Recommendation 2.1 and 2.2.
- Medicinal Product Report Messages to the Report Receiver (EMEA) via physical media following the EWG M2 Recommendation to the ICH Steering Committee for the Electronic Standards for the Transfer of Regulatory Information (ESTRI) Physical Media - Recommendation 2.1 and 2.2.

Before starting the alternative transmission process, the steps indicated below should be followed:

- ***E-mail as Document Transport Choice to the EudraVigilance Gateway***

If the Report Sender is using e-mail as the transport protocol and has not received an MDN for a sent Safety or Acknowledgement Message in over six hours and no rejected Safety or Acknowledgement Message arrived at the Report Sender's Gateway, then there is a possibility that there is a mechanical, programme, electronic or communication failure at the EudraVigilance Gateway at the EMEA. In this case the Sender should contact immediately the EudraVigilance Gateway administrator at the EMEA.

▪ ***HTTP(S) as Document Transport Choice to the EudraVigilance Gateway***

If the Report Sender is using HTTP or HTTPS as transport protocol and experiences connection errors, then the Report Sender should determine if the problem arises at the level of the Report Sender's system, the Internet or the EudraVigilance Gateway. In case the problem cannot be resolved by the Report Sender, he/she should initiate alternative transmissions and if necessary contact the EudraVigilance Gateway administrator.

Since no ICSR-MDN will be generated in this process, the date of the Report Sender's record of sending the physical medium will be sufficient to prove regulatory compliance in an inspection of the Report Sender.

#### **IV.2.2 Failure of message receipt on the processing level**

In case of a database or processing failure after receipt at the level of the EudraVigilance DBMS, the Report Sender may continue to send electronic messages to the EudraVigilance Gateway. This situation will result in the receipt of an ICSR-MDN but not of an Acknowledgement Message. The processing and Acknowledgement of Receipt procedures will be followed as outlined in chapter III once the services at the EudraVigilance DBMS are restored.

All reporting obligations are fulfilled in this scenario. The Report Sender may contact the EMEA administrator to inquire about the missing Acknowledgement Messages if they are not received within two business days. After resolving the failure, all Safety Messages will be processed and the Acknowledgement Messages returned through the EudraVigilance Gateway.

Once the services at the level of the EudraVigilance DBMS are restored, the procedure that verifies the semantics, syntax, format and content both on the message and the report level will be operated again. The Acknowledgment Message will be generated which indicates acceptance or rejection of the received Safety Message(s).

The Report Sender of a Safety Message that has been rejected in part or in total (transmission acknowledgement code 02 or 03) has the obligation to resubmit corrected versions immediately upon receipt of the Acknowledgement Message.

In case of a database or processing failure after receipt at the level of the EudraVigilance DBMS, the Report Sender may also continue to send electronic Medicinal Product Report Messages to the EudraVigilance Gateway. This situation will result in the receipt of an MPR-MDN but not of an Acknowledgement Message. The Acknowledgement of Receipt procedure will be followed as outlined in chapter III once the services of the EudraVigilance DBMS are restored.

### **IV.3. Mechanical, programme, electronic or communication failure at the Report Receiver's side**

In case of any mechanical, programme, electronic or communication failure, which prevents an EDI Partner from receiving any Safety or Acknowledgement Message, the Report Receiver should inform potential Report Sender(s) thereof immediately. In this case the following alternative transmission processes should be used between the Report Sender(s) and the Report Receiver until the services are restored to normal by the Receiver:

- The Report Sender(s) should submit to the Report Receiver a paper report in an internationally acknowledged format (e.g. CIOMS 1). The date of the Report Sender's record of sending the paper report will be sufficient to prove regulatory compliance in an inspection of the Report Sender. The paper report(s) transmitted in an internationally acknowledged format (e.g. CIOMS 1) should be clearly marked with 'FAILURE OF ELECTRONIC SAFETY MESSAGE GENERATION AT RECEIVER'S SIDE'. The paper report will not be processed within the EDI Partner's locally established pharmacovigilance system but only stored for compliance purposes.
- The Report Sender(s) should submit to the Report Receiver the identical data set on physical media following the EWG M2 Recommendation to the ICH Steering Committee for the Electronic Standards for the Transfer of Regulatory Information (ESTRI) Physical Media - Recommendation 2.1 and 2.2 allowing the Report Receiver to load the transmitted data into the local system once the services are restored to normal.

The Report Receiver will inform the Report Sender(s) immediately when the communication failure has been resolved and the regular EDI process can be established again.



## V. Security of Safety and Acknowledgement Messages

To facilitate the secure transmission of Safety and Acknowledgement Messages over the Internet, each party implements and maintains security procedures and measures in order to ensure the protection of Safety and Acknowledgement Messages against the risks of unauthorised access, disclosure, alteration, delay, destruction or loss, ensuring the verification of integrity, the non-repudiation of origin and receipt and ensuring the confidentiality of the Safety and Acknowledgement Message. This includes the installation and operation of applications that allow for the successful transmission and receipt of encrypted and digitally signed Safety and Acknowledgement Messages via the EudraVigilance Gateway, or the use of service providers for this purpose. This software or service necessary to create, transmit, receive, translate, record and store Safety, Acknowledgement and MDN messages must be in full compliance with the documents listed in Annex 4.

The EudraVigilance Gateway uses a combination of public/private key encryption, which is also known as asymmetric encryption and symmetric key encryption. It follows the widely adopted S/MIME standard for securing messages. The EudraVigilance Gateway supports RC2, RC4, DES (Data Encryption Standard) and Triple DES encryption algorithms. Only X.509 certificates are accepted.

For the exchange of Safety and Acknowledgement Messages the EDI partners are operating in a Closed User Group i.e. the parties are known to each other. As a consequence, the parties agree to use the RSA cryptosystem for asymmetric encryption and the digital signatures provided by using certificates. Two types of RSA keys will be accepted:

- Keys issued by a certification authority i.e. managed keys.
- Keys generated by the party individually i.e. self-signed keys.

The following table specifies the algorithm and key lengths for symmetric and asymmetric keys acceptable to the EMEA:

-----  
**Symmetric algorithm for document encryption**

- Triple DES                      168 bits

-----  
**Asymmetric algorithm for authentication**

- RSA                                      1024 or 2048 bits
- 

Dual keys will also be supported.

Before encrypted and signed Safety and Acknowledgement Messages can be exchanged each party must obtain the other's public key. This will be done after each party has created its Gateway profile. Each party generates a self-signed certificate or obtains one from a certification authority. Either way, the process must result in the creation of a public/private key pair for each party. The private half of this key always remains with the party, the public half is provided to the other party.

In order for each party to be connected to the EudraVigilance Gateway, profile information must be exchanged between the EDI Partner and the EMEA. The following items are required for the proper creation of the EDI Partner's profile on the EudraVigilance Gateway:

- Company Name
- Complete Address (Street, City, State, Post Code, Country)
- Gateway Contact Name
- Gateway Contact E-Mail Address
- Gateway Contact Phone Number
- Gateway E-Mail Address for receiving transmissions

The corresponding EMEA-EudraVigilance information is supplied to the EDI Partner.

There are 2 different scenarios for this exchange of information.

- Gateway self-registration if using a product supporting such functions
- Manual exchange of the above information via E-Mail with the addition of the EDI Partner's public encryption certificate

A new certificate must be generated or obtained by each party when

- It becomes evident or it is suspected that a certificate has been compromised
- A certificate needs to be replaced because it expires
- The encryption key is changed at planned intervals

If the use of the above security procedures and measures result in the rejection of, or in the detection of an error in, a Safety or Acknowledgement Message(s) transmission, the Receiver shall inform the Sender thereof, within two business days. The Sender must initiate an alternative recovery procedure following the instructions of the EMEA and resubmit the Safety or Acknowledgement Message(s) until successful completion of this process as outlined in chapter III of this guideline.

## **VI. Recording and storage of Safety and Acknowledgement Messages and Confidentiality and Protection of Data**

All Safety and Acknowledgement Messages must be stored and treated in the same way as other medical documents with appropriate respect for confidentiality. The EDI Message being a Safety or Acknowledgement Message, sent or received should, for the security of the Transaction, be stored completely and in a chronological order, in a secure way and without alteration.

The data transferred using EDI shall be stored in the format in which it has been sent or in the format in which it has been received. This format has been provided as it is the only format of the data, which can be considered as the originally received and will constitute, if necessary evidence of the EDI Message being a Safety or Acknowledgment Message as it has been sent or received, before any alteration of the message has happened.

Following final processing, data should be stored by the Receiver in a dedicated pharmacovigilance information system and data storage should ensure on-line accessibility at all reasonable times. The readability of, and the possibility to print out the messages are criteria that should be complied with. To ensure that readability is maintained, any material, software or any other operational equipment which may be required to access the data and read it, should be retained by the parties, even in the case where updating of systems have occurred. The parties may wish or need, in such cases, to keep the availability of such equipment without retaining it themselves. Such possibility should only be relied on after verification of national/Community legislation requirements. For the purposes of proof and to ensure the readability and reproduction of the EDI message being either a safety or an acknowledgement message, the relevant software should be also maintained accessible.

Conformity of stored data with the initial ICSR, if not received electronically, should be ensured by a quality control procedure, which provides for validation against the original data.

Storage should ensure traceability (audit trail) of all data entered or modified, including dates and sources of received data, dates and destinations of transmitted data.

All Safety and Acknowledgement Messages sent through the EudraVigilance Gateway will be saved for perpetuity in their original form by the EMEA. Incoming Safety and Acknowledgement Messages will be saved in their encrypted and signed format as they were received from the Sender. Outgoing documents will be saved in their original clear text format.

Each party shall safeguard electronic data from tampering and unauthorised disclosure to ensure, at a minimum, the same level of protection as required for their paper equivalents.

This protection must be extended beyond the Transactions to any files or databases that contain information conveyed via EDI. Each party must ensure and provide the security to maintain the confidentiality of the information. When applicable, both parties must also maintain the confidentiality of passwords and other codes required for accessing this information.

It is the responsibility of each party to maintain their own archive of individual Transactions in a format acceptable to themselves.

Furthermore, any services performed by any intermediary in respect of such confidential information shall likewise be subject to the same degree of confidentiality.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995 P. 0031 – 0050) applies accordingly.

## **VII. Technical, organizational and procedural specifications and requirements to operate EDI**

### **VII.1. Technical Specifications**

This chapter describes the computer software and communications standards used by the EudraVigilance Gateway. Senders will be required to adopt hardware, software and data communications configurations to meet these standards, which are based on the recommendations of ICH.

The Sender's EDI system must comply with the following standards for the EudraVigilance Gateway certification:

- S/MIME compatible email system using POP/SMTP, direct connection via HTTP(s) or FTP
- Support for digitally signed MDN's
- X.509 digital certificate support
- EDIINT/AS1 compliance certification or AS2 interoperability
- Direct transmittal of XML documents

The EMEA does not mandate any particular product for the EDI communication. If the Sender's product adheres to the above standards and is fully interoperable with the EudraVigilance Gateway, then the Sender will receive certification from the EMEA to use it. It is the direct responsibility of the Sender to conform to the EudraVigilance Gateway, as the EudraVigilance Gateway is a certified interoperable product.

Communications via the Sender's and the Receiver's Gateway will take place over the Internet. The parties must comply with the full set of the ICH endorsed security standards.

Each EDI Partner is responsible for its own costs of obtaining and maintaining the services of Internet access from an Internet Service Provider (ISP). These costs will include initial hook up charges such as hardware and software components required for connectivity, monthly Internet access rates and any other expenses that may arise from these activities.

### **VII.2. Organizational Specifications**

EDI Partners are responsible for the preparation of Safety or Acknowledgement Messages in full compliance with the documents listed in Annex 4.

EDI Partners, at their own expenses, shall provide and maintain the necessary equipment, software, services and testing necessary to effectively and reliably create, transmit and manage valid Safety and Acknowledgement Messages.

### VII.3. Procedural Specifications

To assure the successful operation of EDI, each new EDI partner who wishes to transmit Safety Messages electronically will undergo a staged test procedure, which includes the following phases:

1. **Communication test** to assure successful Gateway to Gateway communication. The successful completion of the communication testing between the EMEA and the EDI Partner will be certified by the EMEA so that the EDI Partner can move into the subsequent stages of testing.

The process of establishing the connection requires several steps.

- Document Transport Choice
- Exchange of Profile Information
- Exchange of Public keys for encryption
- Testing the Connection

When a successful connection has been established Safety and Acknowledgement Messages can be successfully transferred between each party in the programme. This is accomplished by sending an encrypted Safety, Acknowledgement or Medicinal Product Report Message to the EudraVigilance Gateway, where it is unencrypted, checked for basic accuracy, then re-encrypted and sent to the ultimate destination. A list of appropriate registered parties will be maintained and distributed by the EMEA. Safety, Acknowledgement and Medicinal Product Report Message exchange can only take place between registered parties.

Step 1 of this testing is applicable between all EDI Partners and the EMEA. It is not required between an Applicant, a MAH or a Sponsor and Competent Authorities other than the EMEA, since the EudraVigilance Gateway is the central communication point interlinking all Competent Authorities in the EEA.

2. **Development and validation testing** of EDI partners to the EudraVigilance test environment at the discretion of the EDI Partner. Once the EDI Partner has completed this test phase he/she will notify EMEA/other potential EDI Partners to move into the XML test phase.

Step 2 of the testing is applicable for the testing of all EDI Partners with the EMEA. Other EDI Partners may decide to follow the same step.

3. **XML test phase** with submission of 10 sample cases (Annex 5) to the EudraVigilance test environment with paper reports in parallel to assure the correctness of the XML files and compliance with the requested specifications: syntax, field lengths, minimum information and data coding against ICH E2B(M) and ICH M1 and M2 standard terminology. This will also allow comparison of the submitted data and ensure quality assurance and data consistency. The successful completion of the testing between the EMEA and the EDI Partner will be certified by the EMEA so that the EDI Partner can move into production pilot. The currently established regulatory reporting mechanism will remain unaffected during the test phase.

Step 3 of the testing is applicable for the testing of all EDI Partners with the EMEA. Other EDI Partners may decide to follow the same step.

4. **Production pilot testing** with continuous submission of messages to the production environment of EudraVigilance and parallel submission of paper reports for three months. The EMEA may decide to shorten this period or extend it depending on the outcome of the production pilot testing. The successful completion of the production pilot testing between the parties in accordance with the procedures will be certified by the EMEA. During the test phase the currently established regulatory reporting mechanism will remain unaffected.

Step 4 of the production pilot testing is applicable for the testing of all EDI Partners with the EMEA and all other EDI Partners using their locally established pharmacovigilance system.

5. **Production** with operational electronic transmission of Safety and Acknowledgement Messages without paper reports in parallel may start once all test phases are successfully completed and certified by the EMEA. The EDI Partner declares in writing to the EMEA at which point in time the parallel submission of paper will be discontinued.

Step 5 of the production phase is applicable for all EDI Partners in the EDI process with the EMEA and all other EDI Partners using their locally established pharmacovigilance system.

In the production phase the EDI Partners acknowledge the validity of a Safety or Acknowledgement Message or an MDN, to be the same as an equivalent paper document for all legal and regulatory purposes and will not contest the validity of a Safety or Acknowledgement Message or an MDN effected by the use of EDI in accordance with the terms and conditions of this Guideline on the sole ground that it was effected by EDI.

Any technical changes must be communicated immediately in writing between the EDI Partners. Major technical changes may require the re-initiation of both test phases as described above.

## **VIII. Operational Equipment and Services provided by the EMEA to interested EDI Partners**

The services that EMEA is providing in relation to EudraVigilance will normally be available for accepting Safety, Acknowledgement and Medicinal Product Report Messages 24 hours per day and 7 days per week. The normal business hours of personnel at the EMEA are from 9 to 5 GMT Monday through Friday, excluding public holidays observed by the EMEA.

### **VIII.1 EVWEB**

The EMEA will provide to interested EDI Partners a web based reporting tool, EVWEB.

EVWEB will allow the EDI Partners registered with EudraVigilance to:

- Generate of fully ICH E2B(M) compliant Safety and Acknowledgement Messages and the electronic transmission of these messages in secure way via the EudraVigilance Gateway to any other EDI Partner in the EEA.
- Generate Medicinal Product Report Messages and transmit them electronically in a secure way through the EudraVigilance Gateway to the EMEA where they will be processed and stored in the EVMPD.
- Access EVWEB for query purposes taking into account the access policies agreed at Community level.

To enhance security, digital certificates will be provided for the access of EVWEB. Digital certificates will be renewed at regular intervals. It is the responsibility of the registered EDI Partners and their users to ensure that the digital certificates that secure the access to EVWEB are always valid. The transmission of Safety Messages and Medicinal Product Report Messages through EVWEB will not be able if the digital certificates that secure the access to EVWEB are expired.

EVWEB will also provide access to internationally agreed standard terminology such as MedDRA. EDI Partners will be solely responsible for any license fees that may result from the use of MedDRA within this web based reporting tool provided by the EMEA.

### **VIII.2 WEB Trader**

The WEB Trader is an integrated component of EVWEB. It provides an alternative solution to the use of a local Gateway to support the electronic transmission of Safety, Acknowledgement and Medicinal Product Report Messages. The Web Trader allows registered EDI Partners to exchange EDI Messages with other registered EDI Partners. The Web Trader is only available to EDI Partners, which are not registered as Gateway users in EudraVigilance i.e. organisations that do not have a local Gateway established to support the EDI process in pharmacovigilance.

The message flow using the WEB Trader is outlined in Annex 3.



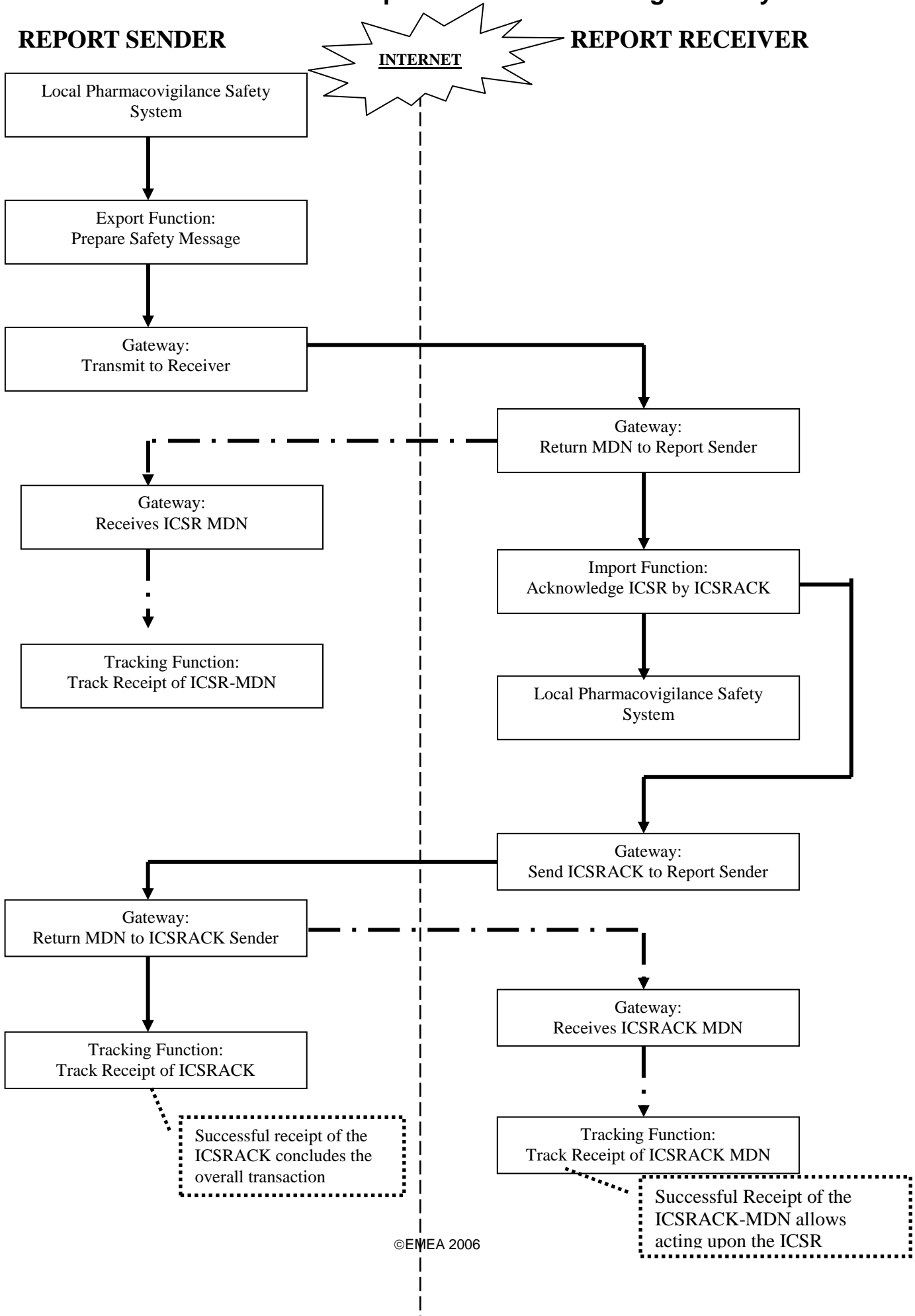
In a WEB Trader Message Transmission a Safety Message can be considered successfully transmitted by the Sender when, after pressing of the 'Send' button, the pop up window in EVWEB displays the notice 'Message sent successfully'. The Sender can confirm the successful transmission by checking the presence of the sent Safety Message in the WEB Trader Outbox.

In addition EVWEB contains tracking functions that enable the EDI Partner registered as WEB Trader to view the date of the transmission of all EDI Messages that have been sent and received.

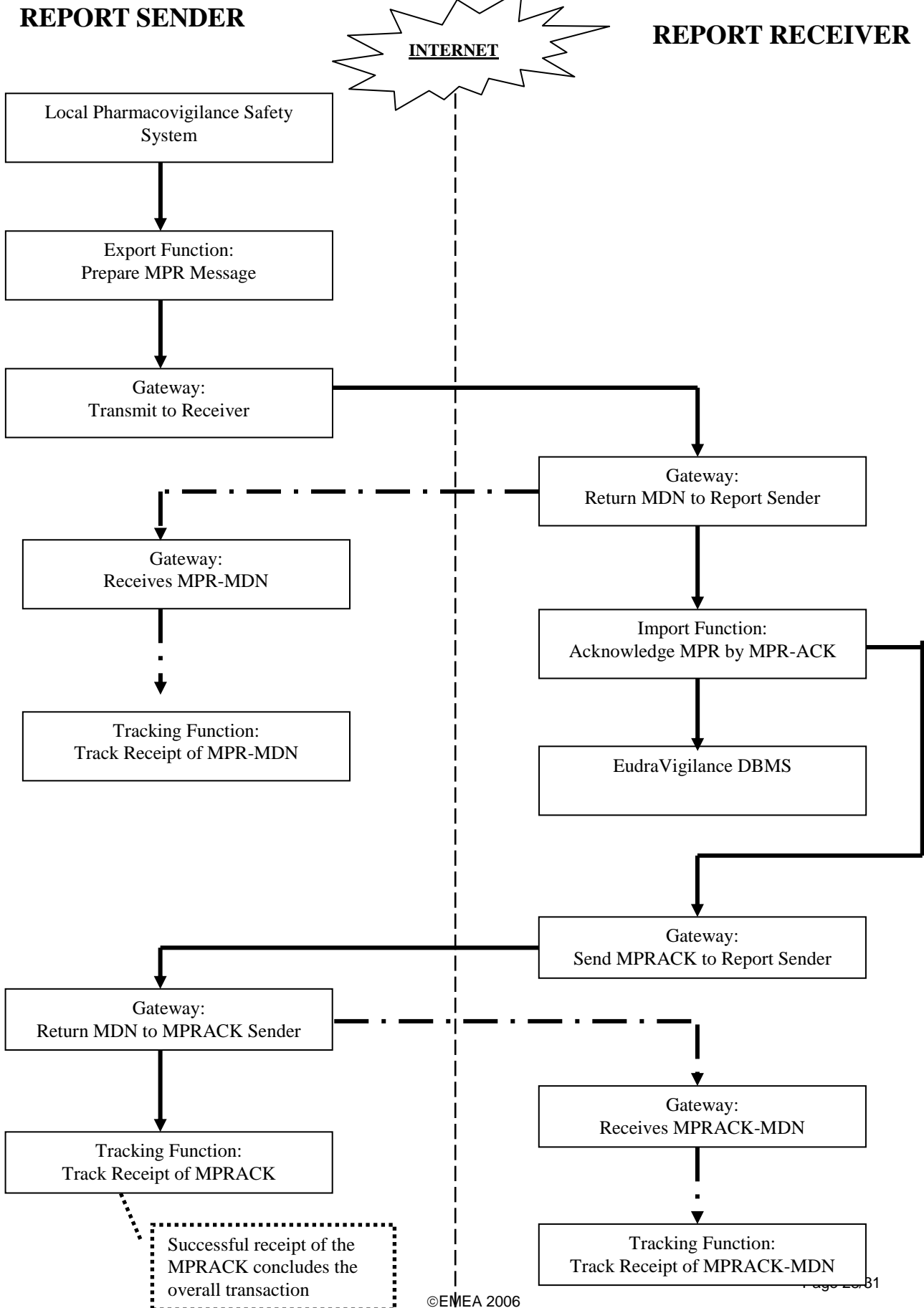
As a general principle, the responsibility for the use of EVWEB and the WEB Trader lies solely with the EDI Partner that subscribes to these services with the EMEA.

**IX. ANNEXES**

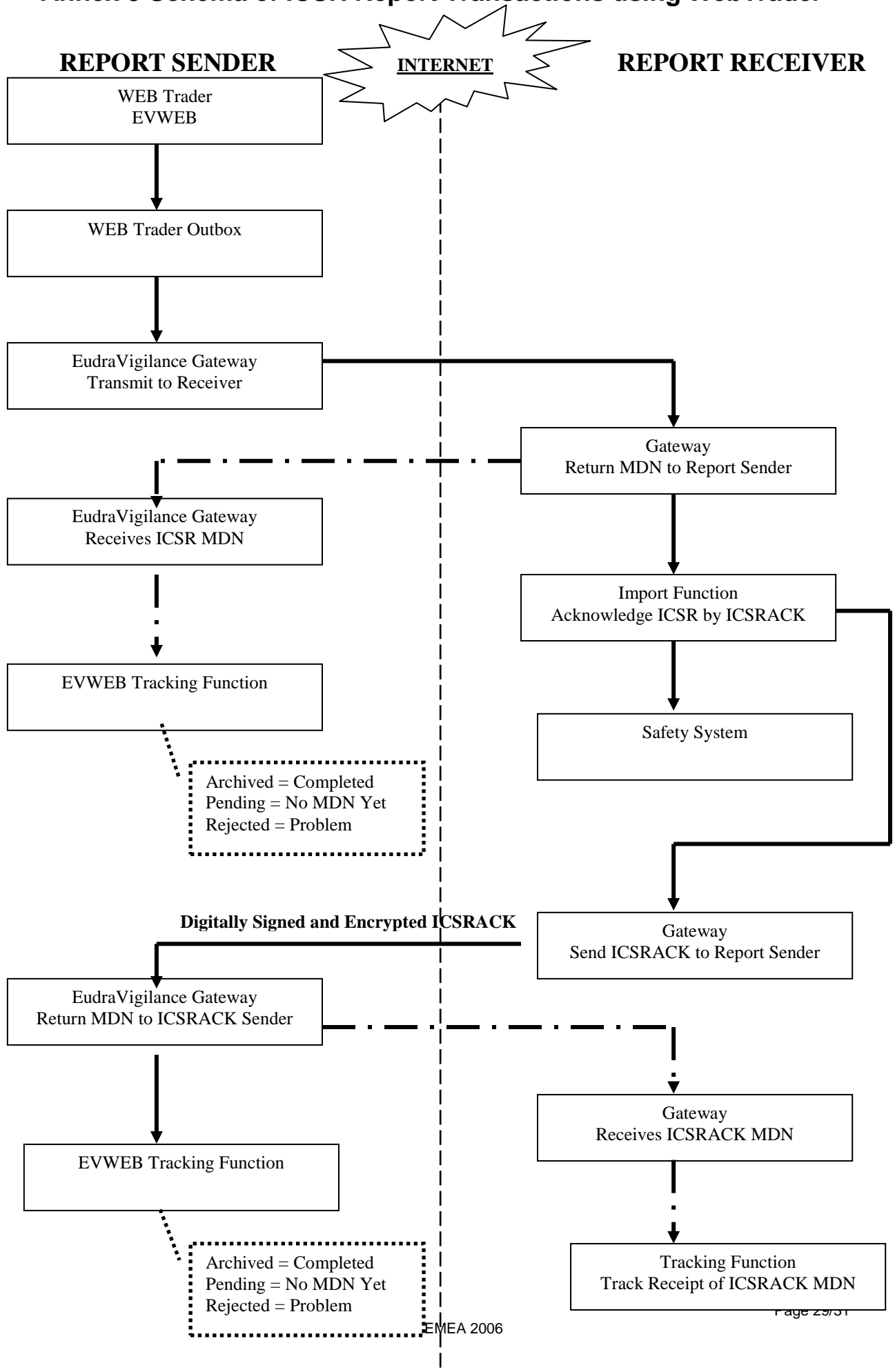
## Annex 1 Schema of ICSR Report Transactions using Gateway



## Annex 2 Schema of Medicinal Product Report Message Transactions using Gateway



# Annex 3 Schema of ICSR Report Transactions using WebTrader



## **Annex 4: Specification Documents Related to this Note for Guidance**

- ICH E2A – Clinical Safety Data Management: Definitions and Standards for Expedited Reporting: October 1994
- ICH E2B(M) – Maintenance of the ICH Guideline on Clinical Safety Data Management: Data Elements for transmission of Individual Case Safety Reports: Version 4.4.1 - 5 February 2001
- ICH E2B(M) Q&A – Implementation Working Group Questions & Answers Version .03, November 11, 2003: Semi-annual releases published at the ICH website <http://www.ich.org>
- ICH E2D – Post-Approval Safety Data Management: Definitions and Standards for Expedited Reporting: November 2003
- ICH M1 MedDRA Term Selection: Points to Consider – Release 3.2, MedDRA version 6.1
- ICH M2 – Electronic Transmission of ICSRs Message Specification: DTD version 2.1: Version 2.3 Document Revision February 1, 2001
- ICH M2 Recommendations
- General 1.1 – Procedure for Recommendations
- General 1.2 – Gateway Recommendation for the Electronic Transfer of Regulatory Information (ESTRI Gateway)
- General 1.3 – Core Standard Set
- Physical Media 2.1 – Floppy Disks
- Physical Media 2.2 – CD-ROM
- Network 3.1 – Messaging
- Security 4.1 – Secure EDI Transmission over the Internet (SMTP/MIME)
- Format 5.1 – Electronic Document Format
- Format 5.2 – SGML DTD Electronic Format for the Exchange of ICSRs (E2B Message)
- Format 5.3 – EDI Header Specification for the E2B Message
- Technical Documentation – EudraVigilance Human Version 7.0 Processing of Safety Messages and ICSRs (Doc. Ref. EMEA/H/20665/04)
- EudraVigilance Medicinal Product Dictionary (Ref. EMEA/H/10488/03)

**Annex 4 with all applicable reference documents will be updated on a regular basis taking into account the continuous evolving technical and scientific standards as defined in the frame of ICH and Community level. This will not affect any other parts of this note for guidance.**

## Annex 5: XML Test Phase; 10 Sample cases

Organisations should provide the following 10 sample cases, which should contain realistic data but do not need to be real cases:

1. Fatal report with cause of death and autopsy sections filled in
2. A follow up report (sent in after the initial report)
3. A report including patient medical and drug history
4. A parent child report
5. A nullification report
6. A report where the worldwide unique safety report number (A.1.10) is either a Regulatory authority's case report number (A.1.10.1) or a Other sender's case report number (A.1.10.2) that is different from the sender's safety report unique identifier (A.1.0.1)
7. A non-intervention study (observational) report sent to EVPM (Receiver ID EVTEST)
8. If applicable to the organisation an interventional study (Clinical Trial phase I-IV) report sent to EVCTM (Receiver ID EVCTMTEST)
9. A case reported in the literature
10. A report with the section report duplicate (A.1.11.1) completed