The European Agency for the Evaluation of Medicinal Products
Post-authorisation Evaluation of Medicines for Human Use

London, 1 March 2002
Doc. Ref: EMEA/H/31387/01/FINAL

Note for Guidance
Regulatory Electronic Transmission of Individual Case Safety Reports (ICSRs) in Pharmacovigilance

DISCUSSION AT THE EUDRAVIGILANCE TELEMATICS IMPLEMENTATION GROUP	NOVEMBER 2001
ADOPTED BY THE EUDRAVIGILANCE TELEMATICS IMPLEMENTATION GROUP	MARCH 2002

Background

This note for guidance intends to assist Competent Authorities in Member States including Iceland, Liechtenstein and Norway and all marketing authorisation holders in the Community in preparing and implementing the electronic transmission of Individual Case Safety Reports (ICSRs) in pharmacovigilance and provides and overview of the procedural and technical steps that need to be followed by all parties involved.

Public

7 Westferry Circus, Canary Wharf, London E14 4HB, UK
Tel. (44-20) 74 18 84 00 Fax (44-20) 74 18 8668
E-mail: mail@emea.eu.int http://www.emea.eu.int

TABLE OF CONTENTS

I. Introduction

This note for guidance intends to assist Competent Authorities in Member States including Iceland, Liechtenstein and Norway and all marketing authorisation holders in the Community in preparing for the electronic transmission of Individual Case Safety Reports (ICSRs) in pharmacovigilance. This guidance will be regularly updated to reflect the latest developments in the area of the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) and the experience gained in the frame of the European Joint Pharmacovigilance Pilot/Implementation activities[1].

The roles and procedures for the expedited reporting of serious adverse drug reactions occurring within or outside the Community are laid down in Community legislation and the relevant Community guidelines. This document discusses general issues related to the electronic transmission of ICSRs, such as file formats, media, transmission procedures and business rules with the ultimate goal of achieving common standards, thereby providing for the best data quality and consistency throughout the Community.

II. General Principles

II.1 ICSRs

For the purpose of this guidance, reports, describing serious adverse drug reactions that need to be exchanged in pharmacovigilance between the various parties in accordance with the Community legislation, are referred to as Individual Case Safety Reports (ICSRs) or safety reports. An ICSR has to contain the data elements as defined in the related guidance documents adopted at international level (please refer to chapter III).
This note for guidance does currently not address the management of ICSR attachments that may accompany ICSRs e.g. scientific literature, as well as other supporting information such as relevant hospital discharge summaries and autopsy/death certificates. Serious adverse drug reactions reported in the literature need to be provided in the structured ICH ICSR format.

Any supporting information related to the case must be sufficiently described within the ICSR with reference to the documents that are held by the sender, which may need to be provided on request.
It is recognised that it is often difficult to obtain all details on a specific case. However, the complete information related to an individual case, that is available to the sender, has to be reported in accordance with the legal requirements as set out in the Community legislation.

This may also include causality assessment if requested by Competent Authorities. It is the responsibility of the sender to structure all information available in accordance with the data elements as defined within the ICH E2B specifications (please refer to chapter III).

[1] Joint Pilot Plan for the Implementation of the Electronic Transmission of Individual Case Safety Reports between the EMEA, National Competent Authorities and Pharmaceutical Industry, EMEA/CPMP/PhVWP/2058/99 rev1.

In addition, whenever more recent information on an individual case is submitted, the complete (entire) information on the case has to be provided and not only partial information e.g. changes or updates.

This does not only apply to the transmission of follow-up information but also if an ICSR is highlighted for nullification. For those ICSRs that are highlighted for nullification ('Report nullification', A.1.13, set to 'yes') also the reasons for nullification must be indicated in detail.

II.2 Electronic transmission format

The electronic transport format for ICSRs has also been agreed upon at international level and is outlined in detail in chapter IV.

II.3 Notification of starting electronic transmission

Before the electronic transmission of ICSRs can be initiated, each party (Competent Authority in Member States as well as Iceland, Liechtenstein and Norway and marketing authorisation holders), who wishes to start the electronic transmission of ICSRs in the Community, must follow the steps as indicated below:

II.3.1 Contact the EMEA co-ordinator

The EMEA Electronic Transmission Co-ordinator must be contacted, who will inform all parties accordingly. Information about the responsible contact person(s) at Competent Authorities in Member States as well as Iceland, Liechtenstein and Norway is available at the EudraVigilance web site http://www.eudravigilance.org

II.3.2 Send Letter of Intent and Implementation Plan

A Letter of Intent for the Electronic Transmission of ICSRs must be sent to the Electronic Transmission Co-ordinator at the EMEA. A template is available at the EudraVigilance web site http://www.eudravigilance.org

In addition, an implementation plan must be provided indicating the approach on the generation and transmission of ICSRs in accordance with the ICH guidelines and the requirements as defined in this document and the steps taken regarding the implementation of the local gateway. The date when the testing of the electronic transmission of ICSRs with the EMEA will be initiated must also be indicated. A template is available at the EudraVigilance web site http://www.eudravigilance.org

II.3.3 Review of the Implementation Plan

The party must discuss its implementation plan with the EMEA Electronic Transmission Co-ordinator. If necessary a meeting can be arranged at the EMEA to outline the specific requirements and to clarify open questions.

II.3.4 Obtain EudraVigilance Gateway certification (for Internet communication)

The EMEA is not mandating any particular software for the electronic communication of ICSRs (please refer to chapter IV.3). If the party's software adheres to the standards as outlined in chapter IV.4 and is fully interoperable with the EudraVigilance Gateway, then the sender will receive certification from the EMEA to use it.

II.3.5 Test phase

Safety reports and safety messages must be prepared in accordance with the requirements as outlined in this document. The party must test the correctness of the XML files before transmission to ensure compliance with the requested specifications: syntax, field lengths, minimum information, data dictionaries compliance (for details please refer to chapter III). The successful completion of the pilot testing between the EMEA and the party, will be certified by the EMEA. During the test phase the currently established regulatory reporting mechanism will remain unaffected.

The test procedures should follow the process as outlined in the Joint Pilot Plan for the Implementation of the Electronic Transmission of Individual Case Safety Reports between the EMEA, National Competent Authorities and Pharmaceutical Industry, EMEA/CPMP/PhVWP/2058/99 rev1.

II.3.6 Signing the Interchange Agreement

An Interchange Agreement specifying the criteria for Regulatory Electronic Transmission of Individual Case Safety Reports (ICSRs) in Pharmacovigilance must be signed. A standard agreement is available from the EMEA.

III.3.7 Operational pilot phase

The operational transmission of safety messages can be started upon successful completion of the test phase. During the operational pilot phase the currently established regulatory reporting mechanism will be further maintained for a period of 3 months, whereby each Competent Authority may decide to shorten this period or extend it. This will allow comparison of the submitted data and ensure quality assurance and data consistency.

II.3.8 Operational phase

Following successful completion of the operational pilot phase, the operational phase will be initiated when electronic transmission of ICSRs will replace the currently established regulatory transmission between the parties who signed the Interchange Agreement.

III. Organising the electronic transmission

The following instructions must be followed to ensure a successful exchange of safety and acknowledgement messages between the EMEA, Competent Authorities in Member States as well as Iceland, Liechtenstein and Norway and marketing authorisation holders in the Community.
Safety and acknowledgement messages have to follow the content and format of the respective ICH guidelines i.e.

- *'Data Elements for the Electronic Transmission of Individual Case Safety Reports' version 4.4.1 dated 5 February 2001.*
- *Electronic Transmission of Individual Case Safety Report Message Specification version 2.3 (ICH ICSR DTD Version 2.1) dated 9 November 2000.*

III.1 Preparation of safety reports (ICSRs) based on the ICH E2BM specifications

Each party is responsible for guaranteeing that the data elements within the locally established pharmacovigilance system are in full compliance with the ICH E2BM specifications. For the preparation of a valid ICSR the following steps must be followed:

III.1.1 Worldwide unique case identification number (A.1.10.1; A.1.10.2)

Section A.1, 'Identification of the Case Safety Report', of the ICH E2BM specifications is designated for the case identification numbers. The ICH numbering convention for these numbers must be followed using a concatenation of country code-sender identification-and report number.

As indicated in the ICH E2BM specifications only the Regulatory authority's case report number (A.1.10.1) or the Other sender's case report number (A1.10.2) should be used. No case and its related case reports should ever have more than one of these fields completed. The contents of whichever item is used must remain unchanged for any transmission subsequent to the original transmission. When a regulator is the initial sender, A.1.10.1 should be used. When an organisation other than a regulator is the initial sender, A.1.10.2 should be used.

When a sender has not previously received a valid ICH E2B/M report electronically, the identifiers (format and content) in A.1.0.1 (Sender's (case) safety report unique identifier) and A.1.10.1 or A.1.10.2 should be identical. Re-transmitters should use their own sender's case safety report unique identifier (A.1.0.1), but not change A.1.10.1 or A.1.10.2.

If an error has occurred the report needs to be nullified.

III.1.2 *Date of receipt of the most recent information for this report (A.1.7)*

The follow up status has not been included in the ICH E2BM specifications as reports can be sent at different times to multiple receivers implying that the report status is dependent on the receiver. The 'date of receipt of most recent information' for this report (A.1.7) together with the worldwide unique case identification number (A.1.10.1 or A.1.10.2) is critical to identify the status of a report. For this reason A.1.7 is mandatory for each report in each transmission.

In the initial report (describing the case for the first time) the field 'date of receipt of most recent information for this report' must be filled in and should contain the same information as the field 'date report was first received from source' if no more recent information is available.
If more recent information is submitted on the case at a later time the 'Date of receipt of most recent information for this report' has to include the date on which the sender actually received the most recent information.

III.1.3 *Coding with MedDRA*

The use of the Medical Dictionary for Regulatory Activities (MedDRA)[2] is required for the entities within a safety report as indicated below.

MedDRA Lowest Level Terms must be provided as either the English term or code until January 2003, when codes only will be accepted. A guidance document on the use of MedDRA versions will be prepared separately.

Section	Data Elements ICH ICSR DTD version 2.1	Mandatory use of MedDRA LLT
B.1 Patient Characteristics	**B.1.7.1a.2 Structured information on relevant medical history**	MedDRA LLTs must be used for the description of the disease/surgical procedure/etc.
	B.1.7.1a.1 MedDRA version for medical history	The MedDRA version must be indicated.
	B.1.8f.2 Relevant past drug history indication	MedDRA LLTs should be used to report the cause of death.
	B.1.8f.1 MedDRA version Indication	The MedDRA version must be indicated.
	B.1.9.2.b Reported cause(s) of death	MedDRA LLTs must be used to report the cause of death.
	B.1.9.2.a MedDRA version for reported cause(s) of death	The MedDRA version must be indicated.
	B1.9.4b Autopsy-determined cause(s) of death	MedDRA LLTs must be used to describe the autopsy results.
	B1.9.4a MedDRA version for autopsy-determined cause(s) of death	The MedDRA version must be indicated.

[2] Marketing authorisation holders can license MedDRA from an international maintenance and support service organisation (MSSO) subscrib@meddramsso.com, Internet at www.meddramsso.com

Section	Data Elements ICH ICSR DTD version 2.1	Mandatory use of MedDRA LLT
	B.1.10.7.1a.2 Relevant medical history and concurrent conditions of parent-Structured Disease/Surgical procedure	MedDRA LLTs must be used for the coding of the medical history in the parent section if applicable.
	B.1.10.7.1a.1 MedDRA version for parent medical history	The MedDRA version must be indicated if applicable.
	B.1.10.8f.2 Relevant past drug history of parent indication	MedDRA LLTs must be used for the coding of the medical history in the parent section if applicable.
	B.1.10.8f.1 Relevant past drug history of parent Indication MedDRA version	The MedDRA version must be indicated if applicable.
B.2 Reaction(s)	**B.2.i.1.b Reaction in MedDRA terminology**	The MedDRA Lowest Level Term (LLT) most closely corresponding to the reaction as reported by the primary source must be provided. In the exceptional circumstances when a MedDRA term cannot be found, the sender should use good clinical judgment to complete this item with the best MedDRA approximation (see MedDRA ™ Term Selection: Points to Consider).
	B.2.i.1.a MedDRA version for the reaction term	The MedDRA version must be indicated.
	B.2.i.2.b Reaction MedDRA term (Preferred Term)	The term can be a sign, symptom or diagnosis. Only the LLT should be provided for electronic transmission in field B.2.i.1.b i.e. B.2.i.2.b must not be completed.
	B.2.i.2.a MedDRA version for the reaction term	This field must not be populated.
B.3 Results of tests and procedures relevant to the investigation of the patient	**B.3.1c Structured Information (tests) relevant to the investigation of the patient**	MedDRA LLTs should be used for the coding of the test and investigation results.
B.4 Drug(s) Information	**B.4.k.11b Indication for use in the case**	MedDRA LLTs must be used for the description of use in the case.
	B.4.k.11a MedDRA version for indication	The MedDRA version must be indicated.
	B.4.k.17.2b If yes to item B.4.k.17.1 (did reaction recur on readministration), which reaction(s) recurred?	MedDRA LLTs must be used to describe recurring reaction.

Section	Data Elements ICH ICSR DTD version 2.1	Mandatory use of MedDRA LLT
	B.4.k.17.2a MedDRA version for reaction recurred	The MedDRA version must be indicated.
B.5 Narrative case summary and further information	**B.5.3b Sender's diagnosis/syndrome and/or reclassification of reaction**	MedDRA LLTs must be used for the sender's diagnosis.
	B.5.3a MedDRA version for sender's diagnosis	The MedDRA version must be indicated.

III.1.4 Medicinal Products

With regard to section B.4, either the 'Active substance name' (B.4.k.2.2) or the 'Proprietary medicinal product name' (B.4.k.2.1) should be indicated. In case both sections are completed, the sender must ensure that the information is compatible in order to avoid generating errors.

Section	Data Element ICH ICSR DTD version 2.1	Required coding
B.1 Patient	**B.1.8a Relevant past drug history**	As for B.4.k.2.1
	B.1.10.8a Relevant past drug history of parent	As for B.4.k.2.1
B.4 Drug(s) Information	**B.4.k.2.1 Proprietary medicinal product name**	For centrally authorised medicinal products, the product name must be provided in compliance with the Community Register of Medicinal Products for Human Use published in accordance with Article 12 of Council Regulation (EEC) N°2309/93, for which the information is part of the EudraVigilance Medicinal Product Dictionary. Medicinal products, which are not part of the Community Register must be submitted in compliance with the WHO Drug Dictionary and/or the EudraVigilance Medicinal Product Dictionary, which will be made available by the EMEA to all interested parties.
B.4 Drug(s) Information	**B.4.k.2.2. Active substance name**	For centrally authorised medicinal products, active ingredients should be provided in English in compliance with the Community Register of Medicinal Products for Human Use published in accordance with Article 12 of Council Regulation (EEC) N°2309/93 for which the information is part of the EudraVigilance Medicinal Product Dictionary.

Section	Data Element ICH ICSR DTD version 2.1	Required coding
		Active substance names, which are not part of the Community Register will be submitted in compliance with the WHO Drug Dictionary or the WHO INN list in English and/or the EudraVigilance Medicinal Product Dictionary, which will be made available by the EMEA to all interested parties.

All marketing authorisation holders in the Community are requested to provide the EMEA with structured information on all medicinal products for which they hold a valid marketing authorisation globally (i.e. in any country within and outside the European Union) content and format to be defined by the EMEA in collaboration with the Joint Pilot/Implementation Group in a separate note for guidance. The same applies to medicinal products where an application for authorisation has been submitted. Marketing authorisation holders/applicants must notify any regulatory changes/updates of the medicinal product information previously submitted to the EMEA immediately to the EMEA in the defined structured format. The information will be made available in the EudraVigilance Medicinal Product Dictionary. The EMEA will treat any medicinal product information, which is still in a process of authorisation, as confidential.

III.1.5 Pharmaceutical form (Dosage form)

Section	Data Element ICH ICSR DTD version 2.1	Required coding
B.4 Drug(s) Information	**B.4.k.7 Pharmaceutical form (Dosage form)**	Dosage forms must be submitted in English according the terminology as defined in the 'Standard Terms on Pharmaceutical Dosage Forms, Routes of Administration and Containers' as published by the Council of Europe.

III.1.6 ICH M2 Numeric Codes for E2BM Units, Intervals and Routes of Administration

ICH E2BM has specified various unit, interval and routes of administration codes for population of certain fields to facilitate efficient data transport, validation and information exchange.

The ICH M2 numeric codes must be used to populate fields that require the E2BM unit list, documented in attachment 1 of the E2BM specifications e.g. B.4.k.5.2 (Dose unit). The three digit ICH M2 numeric codes represent unit measurements for mass, volume, radioactivity, other units and unit intervals e.g. B.2.i.7.1b (Time interval unit between suspect drug administration and start of reaction/event) and B.2.i.7.2b (Time interval unit between last dose and start of reaction/event).

The three digit numeric codes documented in attachment 2 of the ICH E2BM specifications must be used to populate fields that require the E2BM2 routes of administration e.g. B.4.k.8 (Route of administration) and B.4.k.9 (Parent route of administration).

Other field values must be compiled using the controlled codes as reflected in the ICH E2BM specification.

III.1.7 Use of Community Languages

The handling of uncoded information (free text) in different languages is an important issue for the management and the usability of pharmacovigilance information across the EU.
It is therefore agreed that the information in the narrative fields (uncoded information) of safety reports related to adverse reactions

- Occurring within the Community may be provided in one of the official Community languages, whereby English would be the preferred one[3]. If the information in the narrative fields is provided in a different Community language besides English, it is recommended to submit a summary of the data in English.
- Occurring in the territory of a third country will be provided in English.

III.2 *Preparation of safety messages based on the ICH E2B/M2 specifications*

- In order to prepare a valid safety message the following steps must be adhered to:
- The ICSR data must be extracted from the local pharmacovigilance database and a safety message based on the ICH E2B/M2 specifications must be created. There is currently no Commercial Off The Shelf (COTS) Software to convert the data as local pharmacovigilance databases vary in format and structure. The conversion software should be developed in-house or by a contractor taking into account the specific data structure within your local pharmacovigilance database.
- Each safety file must be a well-formed and valid xml file (file extension .xml). The file format must be ANSI (8bit per character) coded with ISO Latin 1 or UNICODE (UTF-16).
- In the ICH ICSR message header the message type of the information being transmitted must be specified. When creating an ICH ICSR safety message, the value of this field should be 'ichicsr'. The message format version and message format release should correspond to the version and release number as specified in the documentation section of the ICH ICSR DTD. The message number is a unique tracking number to a specific ICH ICSR message file transmitted by the sender and is unique to the sender.
- The message sender identifier (M.1.5) must be the sender's own profile ID (please refer also to the EudraVigilance Gateway chapter IV.3 and IV.6) and must be identical with the company or regulatory authority name (A.3.1.2) in each safety report attached to the safety message.
- The message receiver identifier (M.1.6) must correspond with the organisation identifier list maintained by the EMEA please refer also to the EudraVigilance Gateway chapter IV.3).
- Message date and format must indicate when the safety message was initiated.

[3] Note for Guidance on Electronic Exchange of Pharmacovigilance Information for Human and Veterinary Medicinal Products in the European Union, EMEA/CXMP/2056/99.

- The ICH ICSR safety message must include the following XML header
  <?xml version="1.0" encoding="iso-8859-1"?> ANSI latin-1 codification 8bit per character

  or

  <?xml version=”1.0” encoding=”UTF-16”?> UNICODE UTF-16 16 bit per character
- The ICH ICSR safety message must include the following DTD reference DTD version 2.1:
  <!DOCTYPE ichicsr SYSTEM "http://ers.emea.eu.int/dtd/icsr21xml.dtd">
- In the safety message no tags must be used in upper case as in the ICH DTD the tags are all specified in lower case (xml is case sensitive).
- Special characters such as “<” or “&” are represented according to the XML standard and must be avoided in the text. When occurring in the text, they must be replaced by “<”, “>” and “&” respectively.
- The tag structure must be the following:
- <start tag>Value</end tag> [CR][LF]
- Before sending the newly created safety message each party must perform a validation against the reference DTD(s) to be provided by the EMEA when a party is register for the electronic transmission. Only valid safety messages will be accepted.

III.3 *Message and Report Acknowledgement*

An acknowledgement message, as defined in the ICH M2 specifications must be prepared by each receiver and returned to the sender. The objective of an acknowledgement is to verify the usability and compliance of the transmitted data as per ICH recommendations and the business rules as outlined in chapter V). It also permits the sender to track and correct errors, if any, prior to the re-transmission.
The EudraVigilance system will send back an acknowledgment in UNICODE UTF-16 codification.
The Acknowledgment message must report as the message the xml header and the dtd specification.
<?xml version=”1.0” encoding=”UTF-16”?>
<!DOCTYPE ichicsrack SYSTEM "http://ers.emea.eu.int/dtd/ichicsrack11xml.dtd">
NOTE: UTF-16 is the default encoding for XML message if the encoding field is omitted, the message is considered encoded in UNICODE UTF-16.

III. Electronic Transmission through the EudraVigilance GATEWAY

IV.1 *Description of the EudraVigilance Gateway*

The EMEA is in a process of implementing an electronic regulatory submission environment, the EudraVigilance Gateway, that follows the ICH M2 Gateway Recommendation for the Electronic Transfer of Regulatory Information (ESTRI-Gateway). These recommendations require that Regulatory Authorities (EU, US, JP) will implement at least one ESTRI Gateway with pharmaceutical industry and with other authorities that supports secure communication.

The ICH ESTRI-Gateway is defined as a data exchange service, which consists of all core standards and functionality required for supporting the ICH standards (e.g. Simple Mail Transfer Protocol/Secure Multipurpose Internet Mail Extension -SMTP/SMIME- protocol).

The purpose of the EudraVigilance Gateway is to place a single, common, Community-wide reporting gateway into day-to-day operations for receiving regulatory submissions in a fully automated and secure way including all aspects of privacy, authentication, integrity and non-repudiation of all transactions.

It allows marketing authorisation holders to report to a common reporting point within the Community from where the transactions are re-routed to the addressed Competent Authorities in Member States as well as Iceland, Liechtenstein and Norway and the EMEA and the European Commission. It permits Competent Authorities in Member States as well as Iceland, Liechtenstein and Norway a secure reporting mechanism to marketing authorisation holders and the EMEA.
Following the ESTRI recommendations pharmaceutical industry (i.e. marketing authorisation holders) is responsible for implementing at least one of the multiple ESTRI standards in order to ensure electronic communication with any regulator.

The benefits of the ESTRI Gateway implementation for electronic submissions include:

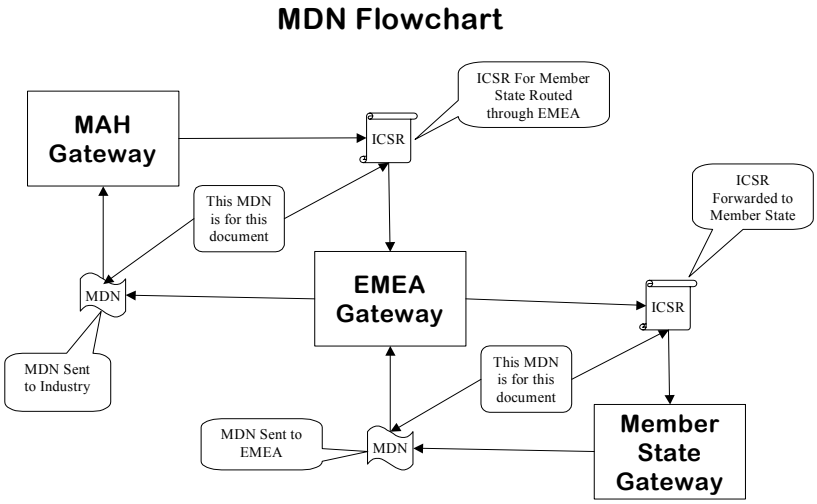
- Standardising data transmission between the EMEA, Competent Authorities in Member States as well as Iceland, Liechtenstein and Norway and marketing authorisation holders,
- Eliminating data transcription errors,
- Reducing paper processing burden/cost for the EMEA, Member States as well as Iceland, Liechtenstein and Norway and marketing authorisation holders,
- Complying with international standards and open technology solutions.

IV.2 *EudraVigilance Gateway Transmission Process*

The "transmission loop" works in the following manner (see figure 1):

- The sender creates a safety message (ICHICSR XML);
- The sender (e.g. marketing authorisation holder-MAH) sends a safety message to the EMEA or a Competent Authority in a Member State, Iceland, Liechtenstein or Norway through it's local gateway compatible with the ICH ESTRI standards to the EudraVigilance Gateway.
- If a safety or acknowledgement message is successfully recognised, decrypted and processed through the EudraVigilance Gateway, an MDN (Message Disposition Notification) is sent from the EudraVigilance Gateway to the sender's gateway. The date of the MDN will serve as the official receipt date of the transmission.
- The EudraVigilance Gateway re-routes the safety message to the indicated receiver.
- The receiver processes the safety message, creates an acknowledgement message (ICHICSRACK) and sends it back to the original sender via the EudraVigilance Gateway.
- The sender's gateway returns an MDN for the receipt of the acknowledgement (ICHICSRACK) message to the EudraVigilance Gateway.

Figure 1: MDN Flowchart



IV.3 *Operational requirements to communicate with the EudraVigilance Gateway*

Each party must provide, all the equipment, software and services necessary to create, transmit, receive, translate, record and store safety, acknowledgement and MDN messages in full compliance with the respective ICH standards and the requirements as defined in this note for guidance.

The EudraVigilance Gateway is providing a single point of contact between marketing authorisation holders and Competent Authorities in Member States as well as Iceland, Liechtenstein and Norway. By doing so, the EudraVigilance Gateway is considered a hub and all connections for both marketing authorisation holders and Competent Authorities in Member States as well as Iceland, Liechtenstein and Norway. Safety and acknowledmgent messages are routed through the hub to the desired spoke. The simplicity of this design allows for the secure transmission of all safety and acknowledmgent messages to every participant without the expense and complexity that would be needed to establish a connection between each and every endpoint. The process of establishing the connection requires several steps:

- Document Transport Choice
  Currently Email for marketing authorisation holders or HTTP and/or Email for Competent Authorities in Member States as well as Iceland, Liechtenstein and Norway
- Exchange of Profile Information
- Exchange of Public keys for encryption
- Testing the connection

When a successful connection has been established safety and acknowledgment messages can be successfully transferred between each party in the program. This is accomplished by sending an encrypted safety and acknowledgment message to the EudraVigilance Gateway, where it is unencrypted, checked for basic accuracy, then re-encrypted and sent to the ultimate destination. The list of registered parties will be maintained by, and distributed by the EMEA. Safety and acknowledgment message exchange can only be provided between registered parties.

IV.4 *Technical specifications of the EudraVigilance Gateway*

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

The sender's gateway must comply with the following standards for the EudraVigilance Gateway certification:

- S/MIME compatible email system using POP/SMTP protocols
- Support for digitally signed MDN's (message disposition notification)
- X.509 digital certificate support
- EDIINT/AS1 compliance certification
- Direct transmittal of XML documents

The EMEA is not mandating any particular software for the electronic communication of ICSRs. If the sender's software 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.

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 party is responsible for the costs to obtain and maintain the services of Internet access from an Internet Service Provider (ISP). These costs will include initial hook up charges, like hardware and software components required for connectivity, monthly Internet access rates and any other expenses that may emerge from these activities.

IV.5 *Processing and acknowledgement of receipt of safety messages*

A safety message must be processed by each party as soon as possible after receipt, but in any event, within two business days once the transaction reaches the EudraVigilance Gateway, is successfully decrypted, recognised, validated and has been successfully re-routed to the actual receiver as defined in the safety message header.

For the successful completion of the process of decryption, reference should be made to chapter IV.6.

A safety message is successfully recognised and validated when

- The sender and the receiver could be correctly identified in the safety message header i.e. both the sender and the receiver must be a registered party of the EudraVigilance Gateway,
- The safety message is well–formed i.e. a valid XML file in full compliance with the requirements as set out in this guidance. The aim of this checking is to evaluate if the received safety message is a correct Extensible Markup Language (XML) message, a subset of SGML that is completely compatible with SGML thereby allowing generic SGML to be served, received and processed on the web in the way that is now possible with Hypertext Markup Language (HTML).
- The safety message is in accordance with the ICH ICSR Document Type Definition (DTD) 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.

It is the sole responsibility of the sender to ensure that the above criteria are fully met and that the safety message can be recognised successfully by the EudraVigilance Gateway.

If the safety message is recognised successfully, an MDN will be returned to the sender, the date of this MDN will serve as the official receipt date of the submission by the EudraVigilance Gateway.

After receipt of the safety message the EudraVigilance Gateway will re-route it to the receiver indicated in the safety message header, this process is to be regarded as successfully completed following the return of an MDN to the EudraVigilance Gateway.

Following the successful delivery of the safety message, the receiver is responsible to load the ICSR(s) into the locally established pharmacovigilance system. Further, the receiver is responsible to generate within two business days an acknowledgement message, providing the status of each ICSR subject to the safety message of the particular transmission. This acknowledgement message must be sent via the EudraVigilance Gateway to the original sender.

In case the transmission status of one or more ICSRs of one safety message is acknowledgement code 02 (ICH M2 Electronic Transmission of Individual Case Safety Reports Message Specifications ICH ICSR DTD Version 2.1) i.e not successfully loaded in the receiver's pharmacovigilance database, the sender has to retransmit the corrected ICSR(s) within two business days.

An ICSR can only be regarded successfully delivered if the transmission status is acknowledged by the receiver with acknowledgement code 01 i.e. it has been successfully loaded into the receiver's pharmacovigilance database. It is the sole responsibility of the sender to initiate the transmission of the same ICSR(s) again until successful acknowledgement (ACK code 01) of this report. An ICSR must be acknowledged as ACK code 01 when it is in fully compliance in format and content with this guidance document.

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 to ensure that these criteria are met and that the acknowledgement message can be recognised and routed successfully by the EudraVigilance Gateway.

If the acknowledgement message will be recognised successfully, an MDN will be returned to the sender, the date of this MDN will serve as the official receipt date of the submission by the EudraVigilance Gateway.

If the sender does not receive the acknowledgement of receipt within two business days, the sender must regard the safety message as null and void at the expiration of that time limit and initiate the transmission of the same safety message again until successful receipt of the acknowledgement message generated by the receiver.

IV.6 *Security Aspects*

To facilitate the secure transmission of safety and acknowledgement messages over the Internet, each party, at its own expenses, has to purchase, install and operate applications that allow for the successful transmission and receipt of encrypted and digitally signed safety and acknowledgement messages via the EudraVigilance Gateway. The applications chosen by each party must provide the essential functionality and interoperability as outlined in chapter IV.4.
Encrypting and digitally signing safety and acknowledgement messages by using certificates provides the parties the following assurance about each transaction:

- Only the receiver can read the message and not any unauthorised party;
- The safety or acknowledgement message cannot be tampered with i.e. data cannot be changed, added or deleted without being noticed. Creating a hash of the original document and signing it with the sender's private key enables this. Before being accepted by the gateway the document is unencrypted, rehashed and compared to the original. If the original hash and the rehash are not identical, the document is assumed to have been corrupted and it is rejected. A notification is sent to the original sender.
- The Sender is, genuinely who he claims to be, which is assured by the message's digital signature.
- The parties cannot claim they did not receive a safety or acknowledgement message. This is referred to as non-repudiation of receipt.

The EudraVigilance Gateway uses a combination of public/private key encryption, which is also known as asymmetric encryption and symmetric key encryption. This hybrid system uses the best characteristics of each method and minimises the shortcomings of each. 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 and only accepts X.509 certificates.

For the purpose of the electronic transmission of ICSRs in pharmacovigilance the parties 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 summarises algorithms and key lengths for symmetric and asymmetric key lengths, the level of encryption to be determined by the sender when the sender's gateway being certified by the EMEA:

Symmetric algorithm for document encryption

- RC2 and RC 4 40 bits, 64 or 128 bits
- DES 56 bits
- Triple DES 168 bits

Asymmetric algorithm for authentication

- RSA 512, 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 it's 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.

Each party, not yet set up at the EudraVigilance Gateway, must export its gateway profile[4], which includes the party's certificate, to a file and send that file by secure means to the EMEA.

If the party is using the same software for transmission as used by the EudraVigilance Gateway, the profiles can be exchanged without manual intervention, all information necessary for connection is contained within the exported profile.
If a compatible solution is used, then the following information, along with the public key must be sent to the EMEA so that a profile can be generated for the partner. This information includes contact name, address, phone number, email address, security settings being used, email address that will receive the encrypted documents. The EMEA will provide this same information to the partner so that an EMEA profile can be created on their system.

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

- It has become 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,
- There is a need to set up an additional sender profile.

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 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. The process is successfully completed if the criteria as outlined in chapter V are met.

[4] Please refer to Annex 1 for the configuration example of a gateway profile

IV. Data processing in EudraVigilance

The following chapter describes the processing and management of safety messages and safety reports by the European pharmacovigilance system, EudraVigilance and some important standard procedures.

V.1 *Data Validation*

Data validation is crucial to ensure data quality and data consistency in particular in the light of an automated electronic data exchange in pharmacovigilance where several thousand of safety reports will need to be managed on an annual basis. Non compliance with the validation procedures as outlined below, may generate errors or warnings. These errors or warnings will be notified to the sender if the EMEA is the receiver allowing the sender to correct these errors and re-transmit the safety message and its attached safety reports.

V.1.1 Well-formed parsing validation

The safety message is validated against its well–formedness i.e. if it is a valid XML file in full compliance with the requirements as set out in this guidance. As outlined in chapter IV.5, the aim of this checking is to evaluate if the received safety message is a correct XML message.

V.1.2 DTD validation

This validation aims to check if the safety message is in accordance with the ICH ICSR Document Type Definition (DTD) (i.e. the message instances, which define each element of the ICSR being transmitted and how the various data elements are related to each other).

V.1.3 Integrity validation

In a next step the safety message instances are checked in accordance with the integrity (field lengths, field types, field values of on the ICH ICSR DTD version 2.1) and business rules in accordance with the ICH E2BM and M2 specifications and the requirements outlined in chapter III.

V.2 *Report Classification*

Once the data validation is completed successfully, safety reports that are part of a safety message, are automatically classified and finally loaded within the EudraVigilance system if the EMEA was specified as receiver. Classification is based on the ‘Worldwide unique case identification number’ (A.1.10.1; A.1.10.2), the ‘Date of receipt of the most recent information for this report’ (A.1.7) and the ‘Report nullification’ (A.1.13) (please refer to chapter III.1). The outcome of the classification is notified to the sender via the acknowledgement message.

Five classifications are possible:

Case report (CR): This is the report containing the most recent information that has been reported for an individual case.

Replaced report (RR): This is the report on an individual case that has been replaced by a follow up report i.e. a report that contains the same ‘World wide unique case identification number’ but with a more recent info date.

Nullified report (NR): This is a report where the 'Report nullification' (A.1.13) is set to 'yes'. It replaces the report with the same 'World wide unique case identification number' and nullifies the individual case.

Duplicate report (DR); This is a report that contains the same 'World wide unique case identification number' and the same the 'Date of receipt of the most recent information for this report' as a Case report already existing in the EudraVigilance database.

Error report (ER): This is a report that did not pass the integrity validation as outlined in chapter V.3. This report will be maintained until the sender provides the corrected report in accordance with the requirements as set out above.

The algorithms for the case classification within the EudraVigilance system can be described as follows:

CN: 'Worldwide unique case identification number'

RD: 'Date of receipt of the most recent information for this report'

NF: Report nullification' is set to 'yes' (1)

LR: loading report (the one that is being loaded)

PR: pre-existing report (any case report existing in the database)

= equal to

/= not equal to

< smaller than

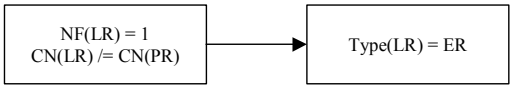
> larger than

An example for the case classification algorithm is presented in figure 2.

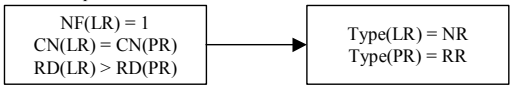
Figure 2: Case Classification Algorithm

Algorithm for EudraVigilance Case Classifications

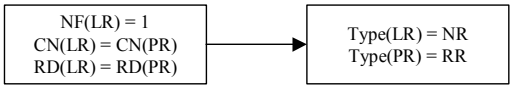
Nullification Reports



Nullification Flag is 1 and Case Number not in Database, then an Error Report is created



Nullification Flag is 1, Case Number in Database and Receipt Date is greater then both, Nullification and Replaced reports are created



Nullification Flag is 1, Case Number in Database and Receipt Date is equal, then both a Nullification and Replaced reports are created

Nullification Flag is 1, Case Number in Database but Receipt Date is less, then an Error Report is created

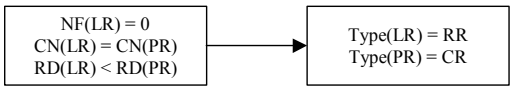
New Reports

Nullification Flag is 0 and Case Number not in Database, then Case Report is added to Database

Follow Up Reports

Nullification Flag is 0, Case Number in Database and Receipt Date is greater, then both a Case and Replaced Report is created

Nullification Flag is 0, Case Number in Database and Receipt Date is equal, then both a Case and Duplicate report is created



Nullification Flag is 0, Case Number in Database and Receipt Date is less, then both a Replaced and Case report is created

Annex 1

Configuration of an Organisation Profile

The following process describes the connection to the EudraVigilance Gateway if a party uses the same software solution as the EMEA.

- Install the software solution.
- Create the profile for your organisation.
- When you choose an Organisation ID for the gateway profile it is recommended to use a string formed by upper case letter or number set (A-Z|0-9). Try to limit the Organisation ID to a maximum of 10 characters. This will limit problems with some email servers.
- Complete the necessary fields when you create the company profile, confirm your entry and your profile will be saved. If you do not complete all fields within your profile, this may generate errors.
- Complete all fields on the Identity Tab.
- The software is capable of sending Alert and Notification messages to a person or group responsible for the maintenance of the server. Enter the e-mail address of this person or group in the appropriate fields on the Preferences Tab. In addition, enter the name of your mail server in the SMTP Server field.
- Configure the Inbound Transports Tab
  - Select the **E-mail Tab** and **POP Tab** as the transport. Check the box marked "**Receive via POP**". This must be a dedicated email account that will be used for sending and receiving safety and acknowledgement messages only. Do not use your own personal email address as the system will retrieve and delete all email in this account.
  - You will need the name or IP address of the mail server, as well as the User ID and password of the new account. Please enter this information in the appropriate fields.
  - On the **XML Tab** insert the following information in order to retrieve the sender and the receiver ID's in the document:

    document type: *ichicsr*
    sender: */ichicsr/ichicsrmessageheader/messagesenderidentifier*
    receiver: */ichicsr/ichicsrmessageheader/messagereceiveridentifier*
    Click on the **Add button**

    document type: *ichicsrack*
    sender: */ichicsrack/ichicsrmessageheader/messagesenderidentifier*
    receiver: */ichicsrack/ichicsrmessageheader/messagereceiveridentifier*

    Click on the **Add Button**

    Make sure that the information is entered correctly, if it is not, there will be errors in the sending and receiving of documents.

- Now save your profile by clicking the OK Button at the bottom of the screen.
- You will be asked if you would like to set up a certificate for your organisation. Click the YES button.
  - You do not need to change or enter any information, click the **Next button** until you see the **Finish Button**, Click **Finish**.
  - You should receive a message stating that the generation was successful.

- You are now at the main Administrator Window.
- Please select Tools and Preferences.
- Select the Outbound SMTP Tab.
- Enter the Name or the IP address of your email server and click OK.
- You are now ready to export the profile of your organisation.
- Make sure that your Company profile is highlighted in the window.
- Select File and Export.
- The profile name will be the default for the name of your organisation.
- Click Save. The profile will be saved in your interchange/profile directory.
- Send your profile by e-mail to the EMEA.
- EMEA will return it's EudraVigilance Gateway profile and the profile for all other stakeholders registered with the EMEA to you.
- Save the profiles to a floppy disc.
- Install the EudraVigilance Gateway profile and the other stakeholder profiles in your system.
- Insert the floppy disc in the system running the chosen software.
- Start the Administrator program.
- Click on Partner Profiles.
- Select File and Import.
- Navigate to the location of the EudraVigilance Profile and select it.
- You will receive a message that the import was successful.
- Configure your gateway for re-routing of safety and ACK messages:
  - Edit EudraVigilance profile.
  - Select the **Secondary Tab**
  - In the **Additional Secondary ID** field enter a *
  - Click the **Add button**
  - Click the **OK button**

- Exchange safety and/or acknowledgement messages with the EudraVigilance Gateway.
- Place the safety and/or acknowledgement messages in the folder:
  - Software>data->(your profile id)->xmlout.
- You will receive safety messages/ ACK messages in the folder:

Software>data->(your profile id)->xmlin.