EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

18 April 2017
EMA/216598/2017
Information Management Division

Information security when using the EudraVigilance system

Best practice guide for management of authorised access to EudraVigilance

The Agency is committed to ensuring the confidentiality, integrity and availability of its information systems and the safety of its assets. Through the adoption of robust controls and best practices, we aim to ensure the continuity of our core tasks and minimise business damage by reducing the likelihood and minimising the impact of security incidents.

In this context we would like to emphasise the responsibilities of stakeholders in relation to the management of their authorised access to EudraVigilance as follows:

General user responsibilities

- user credentials should be unique to each person allowed to access the EudraVigilance system components;
- each user is responsible for the accuracy, the adequacy, confidentiality and the completeness of the information that he/she submits/extracts from EudraVigilance;
- each user is responsible for the use that he/she makes of the information that he receives or extracts from EudraVigilance, in particular for ensuring the confidentiality of such information.

Information handling responsibilities

As a user, you need to:

- ensure the protection of the confidentiality of individual case safety reports (ICSRs) and the rights of the data subjects in accordance with the applicable laws on the protection of individuals with regard to the processing of personal data;
- notify the Agency immediately via the EMA Service Desk [tel. +44 (0)20 3660 7523] of any security breach in relation to personal data transmitted, stored or otherwise protected in connection with data held in or generated from EudraVigilance;
- where no longer required, dispose all confidential information and information related to personal data generated from EudraVigilance in a secure manner, and in accordance with the applicable laws on protection of individuals with regard to the processing of personal data.

Password management responsibilities

As a user, you need to:

- change your password regularly and **never share** your credentials; you should keep your credentials safe;
- use different passwords from the ones you have for your personal accounts (e.g. Gmail, Facebook, Twitter);
- choose **strong passwords** containing a combination of at least three of the following: uppercase and lowercase letters, numbers, symbols (such as ! £ $ % & *);
- ensure your passwords are memorable, so you do not need to share or write them down;
- **not shared your password** by email or with any persons that are asking for it, EMA will never ask for your password.

Organisational measures responsibilities

As an organisation, you need to:

- implement appropriate technical and organisational measures to protect information and personal data, including safety and acknowledgement messages, against unauthorised or unlawful access, disclosure, dissemination, alteration, destruction or accidental loss;
- provide transparent information in your privacy statements on your pharmacovigilance activities regarding the flow of data to EudraVigilance;
- ensure that all computer rooms, communication and information systems in which confidential and personal information obtained or generated from EudraVigilance is stored and/or handled are protected by appropriate security measures;
- ensure that the infrastructure is adequately protected with Antivirus software and that patch management and system vulnerabilities are regularly checked;
- promote security awareness within your organisation against the risk of social engineering and spear phishing by educating and instructing users on recognising malicious emails and sites that are not filtered by organisational technical controls.