Privacy Policy for the Med Safety App for pharmacovigilance

The purpose of this privacy policy is to establish measures to prevent privacy breaches that may occur during the collection, processing, transmission, storage, and use of personal data of patients experiencing adverse effects from taking medication and other health products.

It ensures that all forms of data processing comply with the fundamental rights and freedoms of individuals, adhere to applicable legal provisions on data protection and consider the rights of local authorities, as well as the interests of companies and civil society.

The policy also ensures that the use of Information and Communication Technologies (ICT) complies with the requirements mentioned above and does not violate individual or public freedoms, particularly the right to privacy.

The processing of personal data is strictly confidential. It is carried out only by individuals authorized by the data controller and acting exclusively under their instructions.

The processing of data is conducted by individuals who can assure confidentiality. These individuals must have the necessary technical skills and legal knowledge in data management as well as great personal integrity.

All individuals responsible for processing these data sign a written agreement ensuring compliance with confidentiality.

The data controller is required to take all necessary precautions, considering the nature of the data, to prevent their alteration, deterioration, or any unauthorized access by third parties. These include:

1. Ensuring that, when using an automated data processing system, only authorized individuals can access the personal data relevant to their responsibilities, and that primary personal data is anonymized before being shared with third parties.
2. Verify and record the identity of third parties to whom personal data may be transmitted
3. Allow for the verification and subsequent recording of the identity of individuals who have accessed the information system, as well as the data that has been viewed or entered, specifying the time and the person involved.
4. Prevent unauthorized access to the premises and equipment used for data processing.
5. Prevent any unauthorized reading, copying, modification, destruction, or movement of data storage media.
6. Prevent any unauthorized data entry into the information system, as well as any unauthorized access, modification, or deletion of stored data.
7. Ensure that data processing systems cannot be accessed by unauthorized individuals through data transmission facilities..
8. Prevent any unauthorized reading, copying, modification, or deletion of data during its transmission or the transport of its media.
9. Ensure the backup of data by creating reliable security copies.
10. Update and, if necessary, convert the data to ensure its long-term storage.