INFORMATION SECURITY POLICY

MEDCOR BV · Hooiwegel 14, 9070 Heusden-Destelbergen, Belgium · VAT BE 0712.550.815 · staelshendrik@medcor.be · www.medcor.be

1. Scope

This policy applies to MEDCOR BV (“MEDCOR”), its managing director, associates and subcontractors (“MEDCOR personnel”). It covers all information MEDCOR creates, receives or stores, in particular client documents and personal data, and all systems used to handle it: the MEDCOR Microsoft 365 environment and the devices used to access it, including personally owned devices. It supplements article 10 of MEDCOR’s General Terms and Conditions.

2. Confidential information

All client information is confidential unless the client states otherwise. It is stored only in the MEDCOR Microsoft 365 environment or in systems provided by the client, never in personal email, personal cloud storage, messaging apps or on USB sticks. Data in the MEDCOR Microsoft 365 environment are stored in Microsoft data centres in the European Union. Files are shared only with named persons on a need-to-know basis; “anyone with the link” sharing is not allowed. Paper copies are kept to a minimum and shredded or returned after use.

3. Access

Every person uses a personal @medcor.be account with a strong, unique password and multi-factor authentication; shared credentials are not allowed. Shared mailboxes, such as rip@medcor.be, are accessed only through personal accounts; direct sign-in is blocked and sent items are kept in the shared mailbox. Access is limited to what an assignment requires, granted only after this policy has been acknowledged, reviewed at least once a year and removed within one working day when an assignment ends. Administrator rights rest with the managing director.

4. Devices and email

Devices used for MEDCOR work, including personally owned devices, have disk encryption, supported software with automatic updates, active malware protection and an automatic screen lock after at most five minutes. Mobile devices holding MEDCOR data are protected by a PIN or biometric lock. MEDCOR email is protected by SPF, DKIM and DMARC. Suspicious messages are reported rather than opened or forwarded, and recipients are checked before client data is sent.

5. Client systems, personal data and pharmacovigilance

When a client provides accounts or devices, the client’s rules apply and client data stays in client systems. Personal data are processed in accordance with the GDPR. Adverse event reports and product complaints concerning a client’s products are forwarded to the marketing authorisation holder or manufacturer within 24 hours, or within any shorter timeline agreed with the client.

6. Retention and return of data

Data in the MEDCOR Microsoft 365 environment are protected by Microsoft’s built-in redundancy, version history and recovery of deleted items. Client data is kept only as long as the assignment, the client agreement or the law requires. At the end of an assignment, client data is returned or deleted within 30 days unless agreed or required otherwise; written confirmation is given on request.

7. Incidents

A lost or stolen device, a compromised account, malware, a misdirected email containing client data or any unauthorised access is reported to the managing director immediately. MEDCOR contains the incident and informs affected clients without undue delay and within 24 hours of discovery, or within any shorter timeline agreed with the client. Each incident is recorded with its cause and corrective actions.

8. Subcontractors and continuity

Associates and subcontractors work under a written agreement covering confidentiality, data protection, information security and return of data, and with the client’s consent where the client agreement requires it. Every client-critical role has a named, qualified deputy with access to the relevant shared mailbox and files.

9. Acknowledgement and review

MEDCOR personnel read and acknowledge this policy in writing, by email, before accessing client information. Non-compliance may lead to removal of access or termination of the agreement; exceptions require the prior written approval of the managing director. This policy is owned by the managing director and reviewed at least once a year and after any significant change or incident.