PRIVACY AND INFORMATION SECURITY PRACTICES

for Redcare Pharmacy N.V.

Date | 07.11.2024

Version | 5.0

Confidentiality level | Public

Contents

1. Introduction

Redcare Pharmacy N.V. and its subsidiaries (hereinafter referred to as "we" or "Redcare Pharmacy") is operating in an international environment and is committed to ensure the protection of confidential information and personal data, as well as ensuring compliance with article 12 of the Universal Declaration of Human Rights or article 8 of the European Convention on Human Rights. We are operating in the health sector and are bound to strict laws and regulations in all the countries we do business in. We acknowledge that we process sensitive customer data and information about our customers that need to be well protected and therefore take data security and data privacy, as well as cyber security, very seriously. Redcare Pharmacy recognizes the importance of implementing appropriate technical and organizational security measures in order to prevent any unauthorized access, disclosure, alteration or destruction of such data. For this purpose, Redcare Pharmacy implements industry standard security controls.

This document is not meant to be the internal Redcare Pharmacy Information Security Policy but only serves as a summary of the information security measures implemented for specific business activities.

Redcare Pharmacy security measures follow a risk-based approach and embrace the principles of privacy and security by design.

All measures described hereinafter apply to Redcare Pharmacy and **all** its subsidiaries.

2. Information security strategy and objectives

Redcare Pharmacy's information security strategy aims to achieve the highest possible level of security with the most economical use of resources and the minimization of any remaining risks.

The information security strategy is intended to define, manage, control, maintain and further develop procedures to ensure information security. To further optimize this continuous process, a company-wide information security management system (ISMS), based on the ISO 27001 standard, was developed and implemented. Redcare Pharmacy's ISMS was initially audited by TÜV Rheinland in December 2021, resulting in initial certification without conditions in January 2022.

For Redcare Pharmacy, the following general information security objectives are established based on the ISO27001 standard:

Availability

Systems, applications and data should always be available to authorized individuals as intended.

Confidentiality

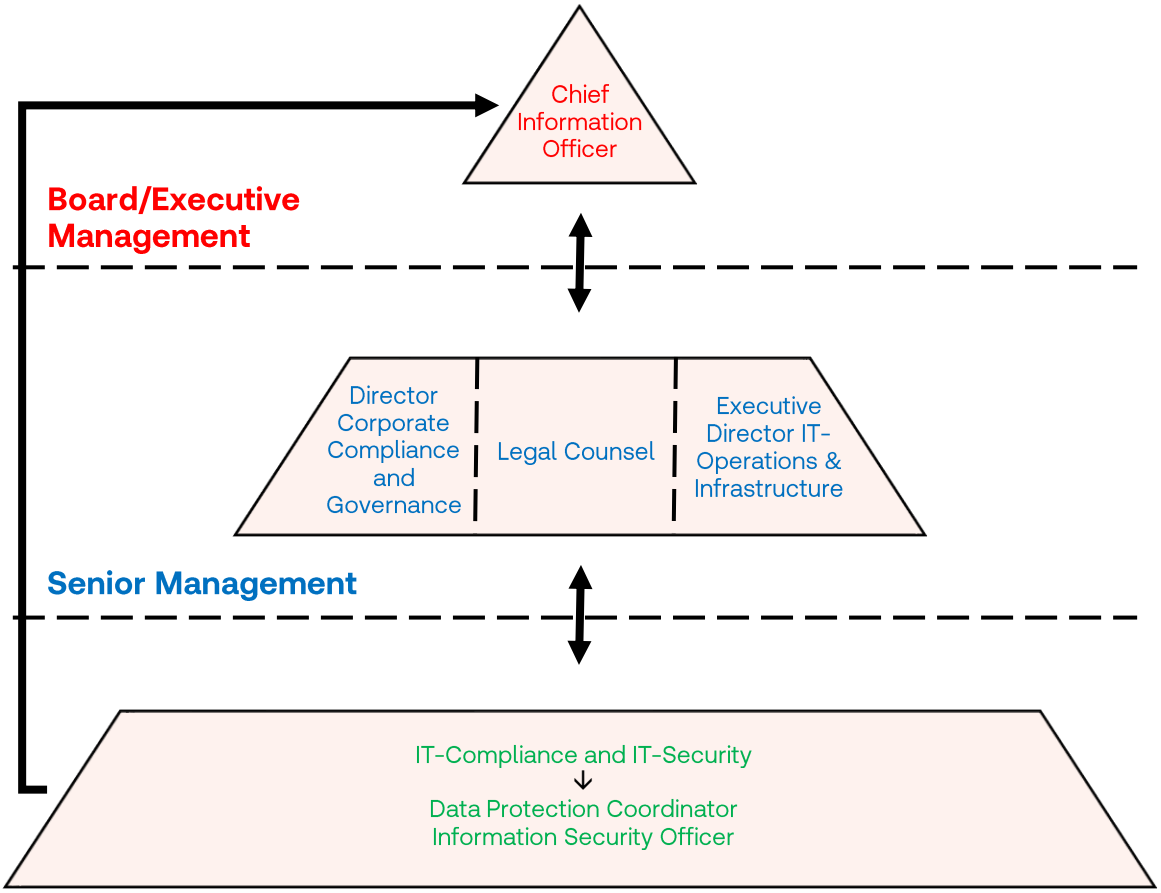
Information must always be protected from unauthorized disclosure. Confidential data and information should only be available to a limited, well-defined, authorized group of people.

Integrity

The correctness of data and the correct functioning of systems should always be ensured. The physical and logical integrity of systems, applications and data should be maintained at all times. This also includes the prevention of unauthorized creation or modification of information.

Next to these general information security objectives, Redcare Pharmacy has defined very specific objectives in its information security strategy, to cover company and industry specific interests and goals in regards of information security and the ISMS, such as acknowledging the reduction of our CO2 footprint or preventing insider threats.

3. Responsibilities and accountabilities



Operational responsibility and approvals

IT-Compliance is responsible for operational activities in the compliance area of information security, including data protection and the development and maintenance of the company's internal ISMS. All operational activities are approved and led by our **Information Security Officer** who directly reports to the CIO.

Guidance

Members of the **Senior Management** hold a supportive function. Should guidance on operational orientation be required, such guidance can be obtained from the responsible members of Senior Management, the Director Corporate Compliance and Governance and the Executive Director IT-Operations & Infrastructure. In the case of legal issues, the Legal Counsel is to be consulted.

Strategic orientation

The responsible member of the **Managing Board (Executive Management)**, the Chief Information Officer, is responsible for the strategic objectives and the definition of the overall strategy of the company in the area of information security and data protection.

The Managing Board (Executive Management) is constantly in close contact with the operationally responsible employees as well as with the members of the senior management. Monthly meetings guarantee the constant involvement of the executive management.

Internal competencies on information security and data protection

Over the past few years, Redcare Pharmacy has exponentially grown and built up broad expertise in information security and data protection to adequately address the increasing urgency and importance of these issues.

This expertise includes, among others, one person who acts as data protection coordinator and five certified data protection officers. Our internal expertise is extended with an external data protection officer.

Three team members who are certified in information security also ensure the maintenance of information security and Redcare Pharmacy's ISO27001-certified ISMS.

4. Certifications and standards

The following certifications and standards have already been obtained or implemented by Redcare Pharmacy:

- Information Security Management System ISO/IEC 27001:2013
- Quality management ISO 9001:2015
- Payment Card Industry Data Security Standard (PCI DSS)
- Guidelines on Good Distribution practice of medicinal products for human use (GDP)
- Respecting OWASP Secure Coding Practices
- General Data Protection Regulation (GDPR)
- IT-Control Framework based on multiple FAIT and oriented towards ITIL
- IT-Governance processes oriented towards COBIT

In addition, a Personal Information Management System (PIMS) in accordance with ISO27701 is currently being developed with the aim of being certified in 2025.

5. Relevant corporate security policies and procedures

The main policies and procedures are listed subsequently hereunder. Additional operational guidelines are in place.

- Information security policy
- Business resumption plan
- IT emergency plan
- Incident management process
- Enterprise risk management system
- Security breach notification process
- Privacy breach notification process
- AI guideline for secure use of AI
- Encryption policy
- Secure Coding Guideline
- Adequate technical and organizational measures
- Transparent data privacy policy

6. Physical and environmental security and technical access control

The access to our premises and our productive environment is monitored through access controls and video surveillance, so that only authorized personnel has access to equipment and information. Asset movement controls are in place for the Sevenum location which location is engineered for seismic, flood and other similar risks. In order to ensure data availability and integrity, cloud services are used for hosting data. All applications and infrastructure used in productive are continuously monitored.

Access to all systems is password protected and granted only to authorized personnel. Password complexity as well as enforced password change are implemented to prevent unauthorized and inappropriate access. Two factor authentication and time-out of system access for remote access is in place.

Redcare Pharmacy uses encryption for data in transit and at rest. Access of system administrators and operators are audited and critical security updates released are installed. Detection and prevention systems are in place to protect network security.

7. Cyber security measures and audits

Redcare Pharmacy has taken many steps to protect itself from cyberattacks and strengthen its own cybersecurity. These include, but are certainly not limited to our long-standing participation in the ethical hacking and bug bounty platform Intigriti, through which we proactively and continuously have our IT systems checked for vulnerabilities by external experts.

In order to meet the requirements of the Payment Card Industry Data Security Standard (PCI-DSS), a vulnerability scan is performed every three months by an external testing agency to check our externally accessible infrastructure.

In addition, we have an all-encompassing penetration test performed at least annually by an external partner company.

Should vulnerabilities be identified, whether via Intigriti, during the three-monthly vulnerability scans or during the annual penetration test, these are addressed and remediated immediately.

Each year, several IT and information security audits are being carried out either performed internally and/or by independent third parties (TUV) resulting in the identification of potential improvements and insights into the maturity of our IT and our Information Security Management System.

8. Data protection and security

To be able to adequately be responsive to all issues arising around the topic of data protection, Redcare Pharmacy has an internal data protection coordinator who, in this position, is responsible for all issues around data security and data privacy. Next to that, an external data protection officer is in place who in close consultation holds an advisory and supervisory function. On the executive level, the Chief Information Officer and a lead pharmacist are responsible for data privacy and security issues.

We do not collect, process or transfer any personal data (including essential and non-essential personal data), without first fulfilling our information obligations or, where needed, obtaining the customers' consent. At Redcare we consider the principles of legality, fairness and transparency in everything we do. In addition, we always try to minimize the data that we collect, economically use and process only data we need and only for the declared purpose. This means that these principles form the basis of all our processes related to personal data. More details on this topic can be found in our privacy policy.

8.1. Data retention

Our customers data will be stored for as long as it is absolutely necessary to achieve the respective purpose for which the data was collected, but for no longer than required by existing legal regulations. It is also possible to restrict processing. In this case, the data will only be stored for as long as the initial purpose is still existent or until the end of the retention period, and will be blocked for all other purposes.

9. Handling of data protection and privacy breaches

If a data protection breach occurs, it is reported internally and documented. In the first instance, the data protection coordinator makes an initial assessment of the breach within 36 hours. The assessment of how to proceed with the breach is based on internally defined and prescribed criteria. If the initial assessment shows that the breach must be followed up, the breach is discussed in a second instance by the Privacy Steering Committee (consisting of CIO, data protection coordinator and legal counsel). A decision will be made whether to report the breach to the Dutch authority and what further actions, such as reaching out to the affected customers or defining a remediation plan, need to be taken. If a decision is made to report the breach, the report is made within 72 hours of the breach. Should communication with affected customers be necessary, either the customer service or the data protection coordinator will take on this task, depending on the severity of the breach. Communication towards media outlets and the press are covered through our Corporate Communication.

In order to prevent future errors and to identify and eliminate possible sources of errors, all data protection errors that have occurred during a month are discussed in a monthly meeting attended by the data protection coordinator, the responsible department and the quality department.

10. Customer data and consumer rights

Redcare Pharmacy is fully compliant with the European General Data Protection Regulation (GDPR) and respects all consumer and customer rights as provided herein. These rights are the following.

10.1. The right to be informed

All customers have the right to know what data is being collected, how it is being used, how long it will be kept and whether it will be shared with any third parties.

All this information is stated in plain language in our privacy policy as published on our website.

10.2. The right to access

All customers can submit subject access requests, which oblige us to provide a copy of any personal data concerning the requester. We will provide this, as required, within one month. Usually, the provision happens within a few days.

10.3. The right to rectification

If customers discover that the information we hold on them is inaccurate or incomplete, they can request that it be updated. As with the right to access, we will fulfill the request within one month.

10.4. The right to erasure (also known as 'the right to be forgotten')

All customers can request that we erase their data in certain circumstances, such as when the data is no longer necessary, the data was unlawfully processed or the data no longer meets the lawful ground for which it was collected. This includes instances where the customer withdraws consent.

10.5. The right to restrict processing

All customers can request that we limit the way we use their personal data.

That can be requested when the customer contests the accuracy of their personal data or when the customer no longer needs the information but we as Redcare Pharmacy require the data to establish, exercise or defend a legal claim.

10.6. The right to data portability

All customers are permitted to obtain and reuse their personal data for their own purposes across different services or request transfer to another service provider. This right only applies to personal data that a customer has provided us as data controller by way of a contract or consent.

10.7. The right to object

All customers can object to the processing of their personal data that is collected on the grounds of legitimate interests or the performance of a task in the interest/exercise of official authority.

10.8. Rights related to automated decision-making including profiling

The GDPR includes provisions for decisions made with no human involvement, such as profiling, which uses personal data to make calculated assumptions about customers or individuals in general.

There are strict rules about this kind of processing, which we are fully compliant with, and all customers are permitted to challenge and request a review of the processing if they believe the rules are not being followed.

11. Interaction and feedback possibilities for stakeholders

Redcare Pharmacy offers various opportunities for different stakeholder groups to get in touch with the company. All these contact options are transparent and publicly accessible.

Customers can contact us at any time either by telephone via our customer hotline or in writing by e-mail. A dedicated e-mail address is available for data protection matters. See also our privacy policy.

12. Human resources security and trainings

12.1. Confidentiality

All Redcare Pharmacy employees are bound to confidentiality and receive all necessary information about the confidential handling of data. The confidentiality is anchored in writing in the employment contract. In addition, a signed letter of commitment is obtained.

12.2. Data protection and cybersecurity training

Each employee receives training on data protection and security, privacy and information- and cybersecurity multiple times a year. The training courses on data protection cover all common and relevant topics of the GDPR and general data protection. In the cybersecurity training courses, all employees are made aware of how to deal with phishing and spam, among other things. Regular phishing tests are carried out, which should reveal whether special training is required for employees. In addition, management and special groups of people with access to sensitive data, such as employees in the HR department, have to undergo explicit training.

We have partnered with leading LMS and training provider *knowbe4* to provide our employees with the best possible training and coaching on data protection and security, privacy and information security. Participation rates are carefully being monitored.

12.3. Process for violations of IT-Compliance requirements

In the event of breaches of IT compliance requirements, sanctions may be imposed in accordance with a defined process. In order to determine an appropriate sanction, the severity and frequency/repetition rate of the breach is first assessed. Sanctions range from verbal warnings to instance dismissal, depending on the severity of the violation. We encourage our people to speak up about violations in line with our Speak Up policy which also enables, as a last resort, anonymous reporting.

12.4. Onboarding trainings

Upon hiring, new employees are assigned to onboarding training, which includes basic training on information security, IT security and data protection. New employees must complete this training within three months, which is carefully monitored. If deficits are identified, the employees are trained individually in the relevant topics. In addition, each new employee is sensitized by our information security officer in a mandatory session.

12.5. Termination of Employment

Upon termination of employment, all access to our IT systems and environments is removed and the company's assets, such as IT hardware, are retrieved.

13. Sub-contractors

Redcare Pharmacy has concluded data protection agreements with its service providers in order to ensure that at least the same level of confidentiality and data security is implemented by its sub-contractors.

Redcare Pharmacy has the right to perform audits in order to monitor the compliance of its subcontractors with the agreed technical and organizational measures regarding data confidentiality and security.

A service provider management system has been implemented to ensure a uniform and rigorous onboarding process for service providers. Potential service providers are thoroughly evaluated with regard to data protection, information security, cybersecurity and IT security as well as general compliance prior to engagement.