knok

Privacy Policy

Privacy is very important for us in knok. This privacy policy describes how we collect and use personal data and circumstances in which we can share this information. This privacy policy applies to the privacy practices of this Internet site, all products or services provided by us and described on the site and other knok interactions with site users. When using the site, additional warnings can emerge on information and information options. You should read these additional privacy warnings to understand how they apply to you.
Visiting or using the site otherwise, is accepting the terms of use of the site and consenting in the collection, use and dissemination practices of knok and other activities described in this Privacy Policy, and any additional privacy statements that can be published in a specific part of the site. If you do not accept and consent, you must interrupt the use of the site, and uninstall all the respective downloads and applications.

Introduction

The Personal Data Protection Policy of knok healthcare, hereinafter referred to as knok, intends to make known to all customers, employees, service providers, or any entity that directly or indirectly relate to this in the context of the development of their activity, the rules and principles of the organisation relating to the protection of personal data. In this way, it is intended to share with stakeholders the data we collect and its purpose, still knowing the measures we take to protect your privacy.

knok thus assumes a rigorous Policy for Data Protection, ensuring that all those who entrust to us their personal data, know how data is treated and what their rights in this matter. The information created, processed and stored by knok, regardless of its support or format, and used during the operational and administrative activities of the business, has to be protected. In this way, information security is based on three essential factors:

1) Confidentiality means that the information is protected against access or exposure to unauthorised entities. Basically, it means that a user should be able to rely that confidential personal information is not accessed by anyone who does not have the rights and a concrete purpose to access the same information. Due to the sensitive information in clinical applications and the amount of data shared through the health ecosystem, confidentiality is assumed as one of the crucial pillars.

2) Integrity means that information maintains all the characteristics defined by your guardian, including control of changes throughout your life cycle. Users should be able to rely that the data to which health professionals have access are accurate and complete and that the prescribed treatment is based on these same data. In the provision of health care the integrity gains even more relevant weight in that a failure in data integrity can result in direct damage to the health of the user.

3) Availability means that information is accessible to authorised personnel whenever relevant. It is about giving access to information when it is required and often in a particular context.
It is also objective of this document to ensure compliance with the applicable legal provisions to bend data protection, in particular in the European Regulation of Data Protection (Regulation No 2016/679 of April 27, 2016) and Law No. 58/2019 which ensures the implementation in the Portuguese legal order of RGPD.

knok

Definitions

For the purposes of this policy and the General Data Protection Regulation (GDPR), it is understood by:
«**Personal data**» means information on a natural person identified or identifiable («data holder»); A natural person is identifiable if it can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, identification number, location data, electronic identifiers or to one or more physical, physiological, genetic, mental, economic, cultural or social identity of this natural person;

«**Treatment**» is any operation or a set of operations carried out on personal data or on personal data sets, by automated or non-automated means, such as collection, registration, **organisation**, structuring, conservation, adaptation or amendment, recovery, consultation, use, transmission disclosure, diffusion or any other form of availability, comparison or interconnection, limitation, erasure or destruction.

«**Responsible for treatment**» means the natural or collective person, the public authority, the agency or other body which, individually or together with others, determines the purposes and means of processing personal data;
«Consent» of the data holder, a free, specific, informed and explicit manifestation, informed and explicit, by which the data holder accepts, by declaration or unambiguous positive act, that the personal data concerning them are subject to treatment;

«**Health data**» means personal data relating to the physical or mental health of a natural person, including the provision of health services, which reveal information on their health status.

«**Minimisation of data**» Principle that it imposes that the personal data collected should be limited to what is necessary for the purposes for which they are treated.
'Violation of personal data' infringement of security which accidentally or unlawful, destruction, loss, alteration or unauthorised access to personal data transmitted or subject to any other type of treatment.

Data Protection Policy

Responsibility for collecting and treatment.
knok is the entity responsible for collecting and processing personal data.
knok's professionals (employees or service providers) are an important element in the life cycle of customer data processing, in so far as, as a rule, they will be those that collect and treat data. The professionals should therefore adopt a set of procedures and caution in the way they manipulate the data in order to ensure the confidentiality of the data and, consequently, avoid safety failures and unauthorised access.

Purpose of Personal Data Collection

knok collects personal data for precise, explicit and legitimate purposes, and will never deal with such data incompatible with these goals. knok uses personal data for customer identification, scheduling and medical services, billing and collection of services provided, satisfaction assessment, complaints and suggestions as well as for other purposes consented by the holder or due to legal imposition.

Personal Data Collection

By collecting personal data, knok informs the holder of the purpose for which they are collected.
At the time of collection knok's professionals ensure the principle of minimisation, ensuring that only personal data is strictly necessary for the act in question. The provision of information on the terms in which personal data shall be guaranteed, through the following elements:
• Entity and contacts of the person responsible for the treatment (KNOK);
• Purpose of treatment;

knok

• Data recipients;
• International data transfer and information in this regard (if applicable);
• Data conservation term;
• Conditions of access, rectification and data elimination;
• Possibility of the holder withdraw the consent;
• Right to submit complaint before the National Commission for Data Protection (NCDP)
• If the holder is obliged to provide the data, and consequences of non-supply;
• Existence of automated decisions (i.e. indication whether the data holder is subject to any decision taken exclusively on the basis of the automated treatment of its data).

What Data do We Collect

Information you provide to us:

• Full name
• Email address
• Phone number
• Date of birth
• Gender (at birth)
• NIF (optional - depends on each country)
• Reason for your query, exams or tests that are marking, session in which you participate, etc.
• Any additional information that has shared or loaded (eg. questionnaires, additional details) during the query markup process.

In the case of health professionals, the following data are collected:

• Full name
• Email address
• Phone number
• Professional ID number
• Personal information published on the Professional Public Profile Page
• Picture
• Details of clinics with which it collaborates
• Any other data provided during the registration process or during the execution of a paid contract.

Information Collected Automatically:

Usage data may include IP address, device identifier, browser type, operating system, information about your site use, and data related to network-related hardware (eg computer or mobile device). The methods that can be used on the platform to collect use data include:

• Registration information: Registration information is given on its use of the platform, such as IP address, browser type, Internet service provider, reference / output pages, date / time records and related data, and can be saved in registration files.
• Information collected by location technologies: Location identification technologies, authentication device, and other location technologies present and developed in the future ("Location Technologies") can be used to collect information about interactions with the site.
• Location Identification Technologies: GPS (Global Positioning Systems) software, geo-filtering and other location detection technologies locate it (sometimes accurately) for the purpose of verifying your location and transmit or restrict content based on your localisation.

knok

Authentication Devices

An authentication device is a unique identifier issued by the operating system of your mobile device.
Although we can access a list of authentication devices, the application and authentication devices do not reveal your identity, the identity of the single device or contact information.

Cookies

Cookies are alphanumeric identifiers that we transfer to your computer's permanent storage medium (or other device) (eg. hard disk) through your browser to allow our systems to recognize your browser and indicate us how and when links of our website are visited and for how many people. We use cookies to improve users' experiences, to learn more about your use of the site and to improve quality. Company cookies do not collect personal data, but we can combine the information collected through cookies with personal data to realize who is or what is your username or email address. Most browsers have an option to turn off the cookies functionality, which will prevent your browser from accepting new cookies, allowing you, in addition (depending on the degree of sophistication of your browser software) decide to accept or not every new cookie in several ways. However, we firmly recommend to leave cookies activated, since cookies allow you to take advantage of some of the most attractive features of our site. Ads that appear on the site can be presented to users by our advertising partners, who can set cookies. These cookies allow the ad server to recognize your computer or other device each time you send you an online ad to compile information about yourself or other people who use your computer or device. This information allows ad networks, among other things, to present targeted ads that might be interesting to you. This privacy policy covers the use of cookies by the company and does not cover the use of cookies by any advertisers.

Use of Advanced Technologies in Data Processing within knok's Services

knok may make use of advanced technologies, including solutions based on Artificial Intelligence, to support the provision of healthcare services through its platform. These technologies may be employed to process and analyse different types of data and content shared by users, with the purpose of extracting useful and relevant information for healthcare professionals in a clinical context. Automated data processing may include, for example, communications, files uploaded to the platform, or other information entered during the use of services. This type of processing will only be carried out when supported by an appropriate legal basis and, whenever necessary, upon the user's prior, informed, and explicit consent.

The use of such technologies is implemented in compliance with applicable data protection and privacy legislation, ensuring full respect for the rights of data subjects. knok adopts appropriate technical and organisational measures to ensure the security, confidentiality, and integrity of the information processed within the scope of these functionalities.

Rights of Personal Data Holders

Under the General Data Protection Regulation, the data holder is guaranteed, the right of access, updating, rectification, treatment limitation or elimination of their personal data, upon request addressed to knok, through the email privacy@knokcare.com or a letter to the address:
knok healthcare - R. Mouzinho de Albuquerque 742, 1º, 4450-007, Matosinhos, Portugal

Access to Information Systems/ Platforms

Health professionals should ensure access reserved for information and platform systems in which health data are recorded. Health professionals should also refrain from duplicating clinic databases by creating, for instance, own files with the database / application information they access.

knok

Registration and Access to Clinical Information

The registration of clinical information of customers should be carried out directly by the health professional. They should only be collected and consequently recorded the data strictly necessary to ensure the provision of medical care. The health professional should only access the client's clinical information in the clinical or other process in so far as it is necessary for the pursuit of their functions.

Sharing Clinical Information

Clinical information should not be shared with third parties except to ensure the continuity of health care provision. In this situation, the professional must ensure that sharing is carried out, securely and confidentially, to another professional subject to the obligation of confidentiality and confidentiality and which follows all measures to protect this sharing of information.

Transportation of Clinical Information

Health professionals should abstain from somehow transporting constant clinical information from the clinical or other process, except in the cases authorised by the institution's guidelines and for the purpose of ensuring the continuity of average care provision. Where special security measures should be adopted, in order to ensure that the information is not accessed by third parties undue (in particular, the information should be anonymised and/ or encrypted).

Use of Personal Devices

The health professional should not use or, in any way, connect personal devices to knok's systems and platforms, except in cases where there is prior approval of the entity responsible. If such happens, and attentive to the nature of the information, the professional must take into account that access to the network through personal mobile devices entails safety and confidentiality risks and should therefore adopt the security measures necessary to protect the data to be, through its device, against destruction, accidental or illicit, accidental loss, amendment, diffusion or unauthorised access, as well as against any other form of illicit treatment of the information. It should also, in any situation, maintain confidential information on secrecy and strict confidentiality, not allowing access to third parties.

Use of Data for Individual Purposes

The health professional cannot treat data collected under the provision of health care for their own purposes. If you want to use the data for academic or research purposes, you must obtain the approval of knok officers and should collect the patient's consent to this purpose by providing you with the necessary information on the terms in which the data will be used. In this situation, the professional will be considered responsible for the treatment of data.

Communication of Personal Data Violations

If any failure occurs or incident involving personal data, the health professional should make communication from it, according to the procedures established for that purpose. In so far as they have information on the incident, they should make it available at the time of communication. In particular, they should communicate the nature of the violation of personal data including, if possible, the categories and the approximate number of affected data holders, as well as the categories and the approximate number of personal data records concerned.

knok

Data Communication to Other Entities

knok will only transmit data to third parties when the data holder requests or authorises or when it comes to a legal imposition. Where there is a need to transmit certain personal data to subcontractors, KNOK will adopt appropriate measures to ensure that the entities with whom the data are shared have implemented safety and data protection measures to preserve their personal data, ensuring they are used according to the previously established purpose. In case of a personal data requirement for auditors or external authorities, their supply will be limited to strictly necessary for these entities to properly implement the tasks and functions that by law or contract are committed to them.

Safety and Good Practice Measures

knok ensures that it will put into practice appropriate technical and organisational measures to protect personal data against accidental or illicit destruction, accidental loss, change, dissemination or unauthorised access, as well as the adoption of measures to ensure a level of protection appropriate in relation to the risks inherent to the treatment and nature of the data to be protected.

• Health information should be of a restricted access to the physician or, under its direction and control, to other health professionals required for professional secrecy.
• When the collection of personal data relating to health is not directly carried out by the health professional (for example, completing a questionnaire directly by the data holder), concrete measures must be taken regarding the movement of this information, which prevent data visualisation per unauthorised person, namely by direct delivery to the health professional or delivery in services, in a closed envelope, addressed to the health professional.
• The clinical record should not contain data on the race, nationality, ethnic origin or information on worker's personal habits, except when the latter are related to specific pathologies or other health data. (cf. Article 109 (3) of Law No 102/2009, of September 10).
• Whenever there is a circulation of network health information, the transmission of data should be encrypted.
• The computerised system must be structured in order to allow access to information according to the different levels of access to users and access to the software access that discipline access permits are assigned. Such passwords must be periodically changed and deleted the user as soon as they stop having access permissions.
• Restricted access, from a physical and logical point of view, should be guaranteed, to system servers, which must maintain an audit registration to sensitive information.
• Backups, should be held in a location only accessible to the system administrator.
• With regard to data contained in paper support, organisational measures will be adopted, which guarantee an identical level of security, preventing undue access and handling.
• In accordance with Article 5 (e) of the GDPR data can only be kept during the period necessary for the pursuit of the purposes of the collection or thereafter.
• The right of information is corollary of the principles of good faith, loyalty and transparency. In this sense, the data holder should be informed of all personal data processing operations and to obtain, at the time of collection of such data, rigorous and complete information of the circumstances of this collection, as set out in Articles 12 and 13 of the GDPR.
• The right of access to the data by the data holder, as well as the right to rectify or request the erasure of your personal data, if applicable, are established by personal data protection legislation. The effectiveness of these rights is essential for verifying the principles of minimisation, accuracy and updating, adequacy and limitation of conservation.
• In accordance with Article 15 of the GDPR, the data holder has the right to obtain access to the personal data treated.

knok

User’s Obligations

Users must, at all times, respect the terms and conditions of the Privacy Policy that is in force and the Agreement on Terms of Use. This includes respect for all intellectual property rights that can belong to third parties (such as images and videos). Users cannot disclose or otherwise disclose any information that can be considered injurious, defamatory, violent, offensive, racist, sexist or xenophobic, or that can otherwise violate the goal and spirit of the site and its community of users. Users cannot provide information to knok and / or other users who believe may be injurious or harmful to their personal, professional or social status. Any violation of these guidelines can lead to restriction, suspension or cancellation of your account by knok, as we take these principles seriously and consider that they are on the basis of membership of our users to the site.

knok reserves the right, at any time, to adjust or amendments to this "Privacy Policy” as such changes are disclosed on their website.