

iPHR

Privacy Statement

Introduction

The iPHR platform is an online system that offers users the opportunity to record, gather, edit, add to, store and share their personal health information. With the iPHR tools, users can control their own personal health record, including how to share their health information with third persons they choose such as their health care provider, family members or friends. More information on all the features of the iPHR and the service it renders can be found in the user's manual. This privacy statement will inform you about the processing of your personal data within the iPHR system and the security measures that have been taken to protect your privacy. In addition to this privacy statement, you can also find special education tools that inform you about the sensitive nature of health data and important points to consider carefully before sharing such data.

How your data will be processed

Your personal information collected through the service will be processed only to the extent that it is necessary to provide the service, and as described in this privacy statement. This service is provided by the Horizon2020 research project iManageCancer. iManageCancer aims to provide novel mobile tools for patients with cancer to empower them and to assist them in managing their disease. These private services are intended for internal tests and clinical validation purposes with project participants and not for public use.

Collection of your personal information and control

Creating an iPHR account is required before using the platform. To create an account, a first time user will be required to provide personal information such as your name, surname, date of birth, gender and e-mail address. Your e-mail address will be used only for the verification of your account, notification in case of change to this privacy statement and for generating a new password in case you forget the one you currently have. If you lose your account credentials you can follow the *lost password* procedure and a new password will be sent to your email. Note that this password is temporary and should be then updated at your next login to the system.

You might be asked for other optional information, but it will be clearly indicated that such information is optional. You can review and update your account information at any time you choose.

You can close your iPHR account at any time by signing in to the service and editing your account profile. When you close your account all your personal data will be deleted according to the conditions set under "Deleting Records"

You will choose what kind of health information to put in your record. Examples of the types of information you can enter include information on:

- **eDiary - Calendar:** A timeline view of all available information showing medications, problems, appointments and procedures.
- **Demographics:** View and update patient information such as gender, date of birth, contact information, name and surname.
- **Labs:** View and update laboratory result values.
- **Problems:** View and update diseases, illnesses, injuries, physiologic, mental or psychological condition or disorders.
- **Procedures:** View and update medical treatments or operations of the patient.
- **Allergies:** View and update abnormal reactions to encountered allergens.
- **Medications:** View and update drugs or other substances received.
- **Measurements:** View and update vital signs that indicate the status of the body's vital functions.
- **Contact:** A form to communicate with other users of the system.
- **Appointments:** View and update appointments between the patient and doctors.
- **Upload Documents:** Upload your health data documents.
- **Assessment app**
- **Psycho-Emotional Status Monitoring**
- **Family Resilience Evaluation Tool**
- **Personal Health Information Recommender:** Allow patients to search in a high-quality document repository for useful information

For a complete overview please check the user manual where you can see all the apps provided by iPHR and the kind of data you can put in your record.

Other information that will be collected to help operate and improve the service refers to how you interact with our services, including the browser that you're using, your IP address, location, cookies or other unique IDs, the pages that you visit and features that you use. We combine this with other users' information to get an overall view of how the service is used.

Deleting entire record

You can delete your personal health record by signing in to your iPHR account and editing your record's profile. Other users that you have given any level of viewing access to your health information will not be able to see your record any longer. After deleting your account, your information is not erased until a period of 90 days has passed in order to help avoid accidental or malicious removal of your health information. Afterwards, your record and the stored information will be permanently deleted.

Deleting health information

When the user moves a piece of health information to the trash, the user can either restore it or delete it permanently from there at any time. Other users with whom the deleted health information has been shared will not be able to see or restore items in the recycle bin, nor can they permanently delete your health information. Permanently deleting health information removes it from the recycle bin. Once an item has been permanently deleted, it cannot be restored. The service adds an entry in your record indicating the date and time that the deletion occurred.

Sharing your health information

The user can share health information with other users or groups called “carenets”. There are three default groups (carenets): Work/School, Physicians and Family. In each of these groups, the user can add as many users as he/she desires. The user will be able to specifically pick those apps and documents stored in those apps that he/she wants to share.

When authorized by you, those persons mentioned in your carenets will only be able to view your data. They cannot change or delete information in your record. Because of the risk to your privacy when inappropriate access is granted to your information, please consider all the consequences carefully before you grant access to any third parties.

Particularly sensitive data can be kept under special restrictions for access. The user can block his account simultaneously blocking all data access to all his/her information.

Security of your personal information

A variety of up to date security technologies and procedures have been implemented to protect your personal information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in accordance with EU Directive 95/46/EC such as:

- encrypting the communication between the browser and the server;
- authentication procedures using a username and a password to receive access to the personal health record;
- comprehensive logging mechanism that ensures that all processing activities taking place within the system are logged and documented;
- replication mechanisms that ensure integrity of data combined with regular internal checks;
- appropriate backup and recovery mechanisms and
- clear and documented instructions on all authorized personnel on how to avoid security risks and breaches

Furthermore, data will be stored in one virtual machine hosted on a public cloud (Amazon Web Services) with the following characteristics:

- data center is located in the EU (Ireland)
- data center is compliant with EU data protection laws
- encrypted storage, the uploaded documents from the patients will be stored encrypted on the server
- provide the following certifications: ISO 27001, ISO 27018

The virtual machine will use the latest version of Operating System with auto updates for security reasons.

Use of cookies iPHR may only use cookies to store the credentials for login purposes

Changes to this privacy statement

This privacy statement may be occasionally updated. In case of material changes to this privacy statement, you will be notified you by placing a prominent notice on the homepage of the p-medicine website and by sending you a notification directly to your email address.

Contact information

In case of any further questions or inquiries concerning this privacy statement, please contact:

Name: Maria Chatzimina

Address: Nikolaou Plastira 100, Vassilika Vouton , GR-70013 Heraklion, Crete, Greece

Telephone number: +30 2810 391672

Email: hatzimin@ics.forth.gr