CaboLabs

Health Informatics, Standards and Interoperability

Acceptable Use Policy

Last Updated: June 20, 2018

CloudEHRServer

This Acceptable Use Policy (AUP) for the CloudEHRServer (the “Service”) by CaboLabs (the “Provider” / “Us”) defines the basic behavioral framework for all the users of the Service, which allows Us to provide an acceptable level of service, in a secure way, while preventing misuse of the Service and unsecure practices.

Violations of the AUP which we consider deliberate, repeated, or represent a risk or harm to other users, other customers, the Service or third parties, may lead to suspension or termination of your access to the Service.

Acceptable Uses:

- comply with all the terms included on this AUP;
- comply with all applicable laws and governmental regulations, including, but not limited to, all intellectual property, data, privacy, security, and export control laws, and regulations promulgated by any government agencies, including, or international organizations;
- use commercially reasonable efforts to prevent unauthorized access to or use of the Service;
- use the Service in a fair way, preventing abuse, and complying with your subscription plan;
- only upload data that you own, control, have the rights of use, or that you are entitled with the custody, management or safeguarding;
- keep usernames, passwords and all other login information confidential;
- monitor and control all activity conducted through your account in connection with the Service;
- promptly notify Us if you become aware of or reasonably suspect any illegal or unauthorized activity or a security breach involving your accounts, including any loss, theft, or unauthorized disclosure or use of a username, password, or account;
- promptly notify Us if you become aware of or reasonably suspect any Unacceptable Uses of the Service; and
- comply in all respects with all applicable terms of the third party applications or services that can be integrated and used form the Service.

Unacceptable Uses:

- share, transfer or provide your personal account information with other person, including username, password or any other data used to access the Service;
- publish private data, including, but not limited to, authentication data, personal data, organizational data, clinical data;
- use the Service to store or transmit any data that may infringe upon or misappropriate someone else's trademark, copyright, privacy rights, or other intellectual property, or that may be tortious or unlawful;

- upload to, or transmit from, the Service any data, file, or link that contains or redirects to a virus, trojan horse, worm, malware, or other harmful component or technology that unlawfully accesses or downloads content or information stored within the Service or on the hardware of the Provider or any third party;
- attempt to reverse engineer, hack, disable, interfere with, modify, or disrupt the features, functionality, integrity, security, or performance of the Service, including any mechanism used to restrict or control the functionality of the Service, any third party use of the Service, or any third party data contained therein;
- attempt to gain unauthorized access to the Service, related systems, networks, or to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection or monitoring mechanisms of the Service;
- access the Service in order to build a similar or competitive product or service or copy any ideas, features, functions, or graphics of the Service;
- use the Service in any manner that may harm other users, customers, the level of service or Us;
- impersonate any person, organization or entity, including, but not limited to, an employee of ours, an “Administrator”, an “Account Owner”, a “Manager” or any other authorized user, or falsely state or otherwise misrepresent your affiliation with a person, organization or entity;
- access, search, or create accounts for the Service by any means other than our publicly supported interfaces (for example, abusing the REST API, "scraping" or creating accounts in bulk);
- sublicense, resell, time share or similarly exploit the Service;
- use the Service for consumer purposes, as the Service is intended for use by businesses and organizations, as the Service is strictly designed for Managers, not for end users including, but not limited to, clinicians, nurses, allied health professionals or clinical technicians;
- use contact or other user information obtained from the Service (including, but not limited to, email addresses) to contact authorized users outside of the Service without their express permission or authority, or to create or distribute mailing lists or other collections of contact or user profile information for authorized users for use outside of the Service; or
- authorize, permit, enable, induce or encourage any third party to do any of the above.

Contacting CloudEHRServer

Please contact us if you have any questions about the Acceptable Use Policy.

Email: info@cloudehrserver.com

Postal Address:

CaboLabs Health Informatics

Juan Paullier 995 apt. 703
CP 11200
Montevideo, Uruguay