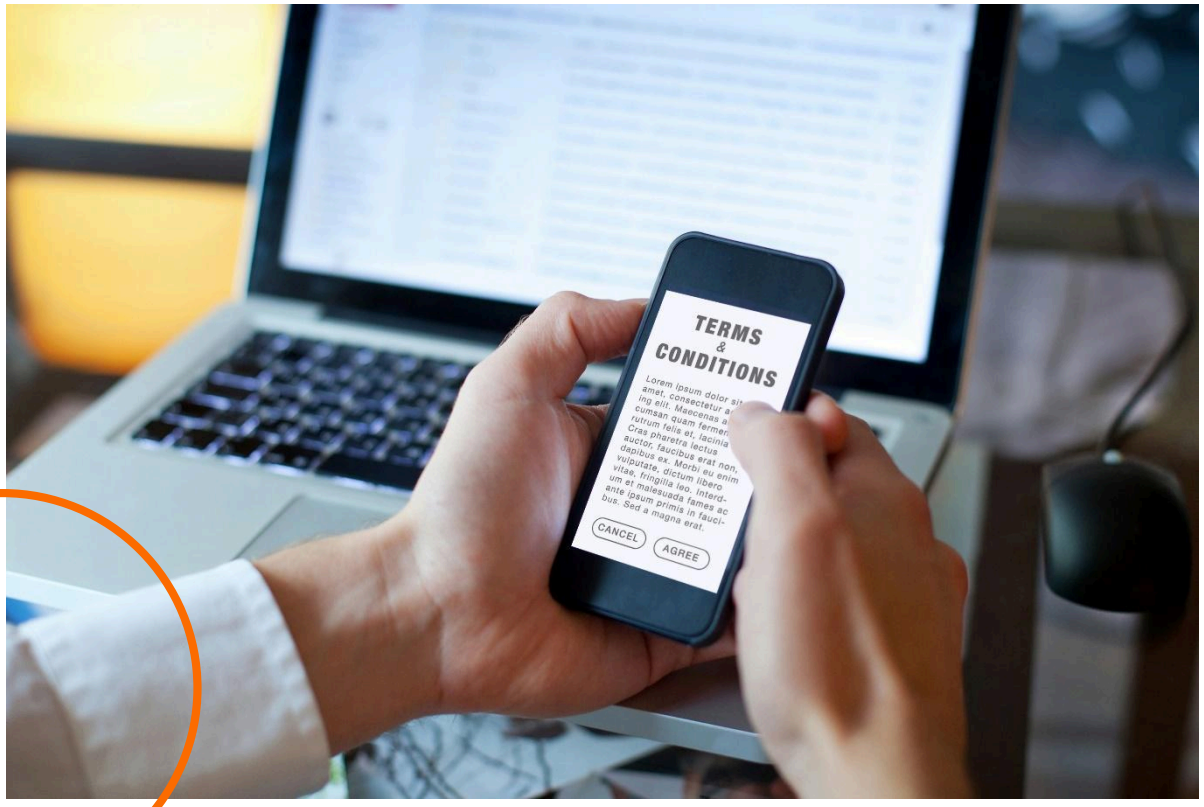
Beacon Medical Systems Ltd trading as Pando

Pando Mobile and Web Acceptable Use Policy

The Pando App – Mutual terms and conditions of use



Purpose: Beacon Medical Systems Ltd (“us”, “we”, or “our”) operates the Pando mobile application (the “Service”). Pando is also a trading name of Beacon Medical Systems Ltd.

Please read these licence terms carefully. You acknowledge that you have read and understood the Agreements, accept these Agreements, and agree to be bound by them.

By using Pando you agree to these General Terms and the Privacy Notice (collectively referred to as "the Terms” The Terms also include a Data Processing Agreement which should be signed by the appropriate person at your healthcare organisation. Please read them carefully. If you don’t agree to the Terms, you can’t use Pando.

Table of Contents

1.1 Introduction

This Acceptable Use Policy (AUP) outlines how the mobile and web applications (Pando) should be used, and defines the mutual responsibilities that exist when using the App.

Please note that this service is not an alternative to the usual professional practices and procedures that you would carry out as part of your professional responsibilities. You should not rely on our service having 100% availability and you must remain properly informed as to the processes and procedures, especially in the light of data protection law and information governance stipulated by the organisation for which you work.

1.2 Purpose

This AUP is in place to ensure that all users of the Pando application are aware of acceptable and unacceptable use of the platform and particularly that personal data is processed legally and/or that patient safety is not put at risk. By downloading and signing up (creating a user account) to use Pando, users agree to comply with the terms of this Acceptable Use Policy and that they have read and understood the Privacy Notice.

Pando operates fto national guidance surrounding IT Safety and best practice (NHS England and Department of Health) by ensuring all systems are assessed for compliance with Information Governance and Patient Safety regulations; users of Pando can find supplemental information on the responsibilities and policies underlying compliance by contacting the Pando team. The Pando team reserves the right to update this document as necessary.

1.3 Scope

This document relates to the use of Pando as an application by all users, in clinical, local government, private and community settings within the United Kingdom.

You should also check if there are any further conditions required by your employer surrounding your use of Pando.

1.4 General Information About Pando

Pando is a secure messaging and workflow mobile application for healthcare and service professionals – this includes doctors, nurses, allied health professionals and service and support staff (e.g., those working in local government). Pando contains features to create and manage lists, organise and assign tasks, initiate video calls (if enabled), share photos and patient profiles with other healthcare professionals, and send instant messages. Pando can be used by anyone with an NHSmail or NHS Trust email address or an appropriate approved secure email domain that has passed due diligence screening -e.g., a .gov address. It is primarily designed for clinical use but is also useful to managers, secretaries and other authorised personnel. Pando is intended to be used by those working in health and social care, local government and private practice, in accordance with their respective professions' own codes of conduct.

Pando reserves the right to remove a user, subject to unacceptable use, or operational requirement at any time.

1.5 Privacy Rights and Responsibilities

Pando's privacy notice can be found here.

1.6 Responsibilities of the User

Please note that internet transmissions can never be regarded as completely private or secure and that any message or information that you send using the App and Service may be read or intercepted by others. All messages are encrypted but this still places a responsibility on you as a medical professional to comply with the following terms of use.

By using this App and the messaging service you confirm that you or the organisation for which you work is a data controller for the purposes of data protection legislation and you acknowledge your legal responsibilities in relation to the personal data sent or received using this service.

1. Pando must not be used to violate any laws or regulations of the United Kingdom or other countries. Any illegal activity will be reported to your employer and to the police.
2. Pando must not be used for commercial gain including any sort of marketing, advertising and/or selling goods or services.
3. Users of Pando must identify themselves accurately and as fully as is necessary to be correctly identified by other healthcare and affiliated professionals using the App.

4. Users are responsible for maintaining their own identifiers including, but not limited to, Profession, Grade, Hospital, Care home, Council and Specialty as laid out in “Settings”. You are responsible for ensuring that any person with whom you communicate is the person that you think them to be (i.e., ensure that they are not using a false identity).
5. You are responsible for checking that the address(es) of the users with whom you interact are correct.
6. In line with data protection legislation and NHS Caldicott principles, you should carefully consider the content of the messages that you send when they transmit personal data. You should keep this to a minimum and only include personal data (e.g., name, age) etc. under circumstances that you think are essential to the other person’s understanding of the message. You should avoid sending sensitive personal data (such as sex life and religious beliefs).
7. You should be careful when you share data outside your own healthcare organisation. If you are sending a message to a clinician in a different organisation to your own it is your responsibility to ensure that there is an appropriate data sharing agreement in place with that organisation. If you are in any doubt, you should contact your own IG Team.
8. The service is intended for transitory communication to facilitate better patient care or improve service delivery but should not be regarded as a permanent record. The service is not intended to supplement or replace official patient/service records or replace your organisation’s official patient/service records. You must update your organisation’s patient record with information relating to the patient’s care that has been determined through the use of this App. The official records must be updated in the usual way with any relevant information communicated using it.
9. In a clinical setting, personal data should only be sent in the course of carrying out your duties as a member of the clinical staff caring for patients otherwise you may risk having no legal basis for which to process that data.
10. You should always comply with your employer’s guidance around information governance and ensure that your messages comply with any guidelines that they have issued.
11. If your employer does not have a data processing agreement with Pando, we recommend following this guidance from NHS England on the use of instant messaging software.
12. Users of Pando must not attempt to interfere with its software, dashboard or databases. Users have an implied responsibility to report any interference with Pando technology to protect personal data and/or promote patient safety.
13. Users must protect their own mobile device from theft or loss; in the event of theft or loss personal data should not be at risk, but the user may be temporarily uncontactable, therefore it is the user’s responsibility to alert colleagues to this and to login on another device as soon as possible.
14. Users must keep their Pando PIN confidential and secure, as well as the password to any email account linked to their Pando account. It is recommended (but not essential) that users also protect their device by touch or PIN identification. We recommend that users avoid the 10 most common PIN combinations and set a PIN that is different to that used to access the device. You must not transfer the App to

anyone else; if you loan your device then you must delete the App first. Users are responsible for all communication that has been made under their password/PIN.

15. If Users opt to use Touch ID either for their device or for Pando, they must ensure that only they have access to the application i.e., no one else has a fingerprint enabled on their device.
16. You must report any breach or suspected breach in the security of your App details to your own Data Protection Officer. Pando's Data Protection Officer must also be informed dpo@hellopando.com
17. Communication via Pando is presumed to be of a professional nature and users should be aware that the content of messages relating to clients/patients may, on occasion, be requested by their employer as part of investigations or audits in their capacity as the Data Controller.
18. Users are responsible, within reason, for seeking support from the Pando team when a technical or other issue arises. Failure to do so could technically result in a breakdown of communication which may put patients or clients at risk. Pando is responsible for providing timely and effective support to users.
19. It is assumed that users who are off duty will set their status to "unavailable". Failure to do so may result in inappropriate attempts to contact an individual and may result in wasted time. Similarly, it is the individual's responsibility to set their status to "available" or "on call" as indicated.
20. Pando may be accessed from off site, depending on individual responsibilities and at the health professional's discretion.
21. Pando is only for people aged 18 years and over. By using Pando, you affirm that you are over 18.

1.7 Information Governance and Security

GMC requirements for doctors and equivalent guidelines for other health professionals state that patient records should be clear, accurate and legible. Pando users are responsible for ensuring that patient demographics are correct to avoid misidentification of patients. Pando is not designed as a replacement for written or electronic patient records and any information recorded on the platform should therefore be duplicated in the official patient record.

Pando is designed for sharing photographs. Consent should always be sought and confirmed before taking a photograph of a patient/data subject, and the health professional should explain its purpose and with whom it will be shared. This consent, and the intended use of the photograph should be obtained and formally documented in line with local information governance guidance. Users must note that the quality of photographs taken within Pando will depend upon the device and will not necessarily meet required quality for diagnostic imaging or medical photography. Photographs taken within Pando should not be used as a substitute for these, but as an adjunct to clinical discussion only and users should always follow local guidance. Where there is an electronic patient record (EPR), then the images obtained through the mobile device should be linked to the EPR and retrievable through it. If a photograph is taken on the phone's camera, then uploaded to the Pando gallery, that photo should then be deleted from the camera roll.

Information from Pando can be directly exchanged with other secure platforms designed to handle Patient Identifiable Information, e.g., NHSmail, but not with outside platforms without prior approval from the data controller.

Pando users must successfully complete annual Information Governance training in accordance with the policy of their own organisation.

Pando has been designed for use in the UK. As such, users that wish to use Pando in organisations outside the UK will need to consult local policies and laws.

Pando users are expected not to send any material by email that could cause distress or offence. In clinical settings, Caldicott Guardian permission must be sought before sending explicit or very sensitive material, as with any other means of communication. It is the user's responsibility to ensure that anyone with whom Patient Identifiable Data is exchanged has a valid reason to receive that data, as per Caldicott principles. Healthcare professionals are free to use Pando in any clinical context; this includes private practice and primary care.

All uses and sharing of confidential personal information that do not have a lawful basis for processing should be treated as data breaches and reported through the usual mechanisms stipulated by your employer's Information Governance, Caldicott and Data Protection Teams.