Privacy Policy 2018

Our Approach to your Privacy

Plus Health Company are committed to taking good care of your personal data and information and will always ask your permission before we store any of your data. Personal information is data that can identify a single person. We require certain information in order to accurately identify you and distinguish you from another person. This is particularly important when working in the healthcare sector. You may wish to visit https://ico.org.uk/ and https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ for further information.

Ultimately, we respect your privacy and promise to treat your information as confidential. We would only ever disclose confidential information if:

- ✓ We have your permission
- ✓ The law allows
- ✓ It is in the client's best interests or:
- ✓ It is in the publics best interest (to protect public safety or prevent harm to others)

It is important to us that we earn and maintain your trust and promise only to store necessary data which enhances your customer experience and is required by professional obligations and in law. We promise we will never sell or share any of your data with a third party, outside of those directly related to how we run our company. For further details on this, please see the following sections:

What Data we Store & Where

Telephone: To assist the day to day running of the company and to enable us to get in touch easily, we store your name and telephone number within the company mobile phone and may make telephone calls to you intermittently. When leaving a voicemail message, we will only state where we are calling from and request a call back. We promise not to disclose any further details about the reason for our call.

We will also use your telephone details to send text messages/imessages as and when required. For instance, to inform you about a class/appointment cancellation at short notice. Once we have dealt with text/imessage or voicemail, whether sent by us or you, we will delete this from our inbox.

Your name and telephone number will also be stored in our online booking system called mindbodyonline. It is important to us that we can reach you, should we need to get in touch. For further details on the data we store in mindbodyonline, please see below.

Email: Company email is provided by Microsoft Outlook. Staff emails are provided via gmail.com. Communications sent between members of staff and third parties which include identifiable personal data will be sent encrypted via Egress Switch (with your prior consent).

We may email you directly from the hello@plushealthcompany.co.uk account (primarily to send registration paperwork, information leaflets, outcome measures) and via automated email from the mindbodyonline or Constant Contact programs (see below).

Plus Health Company will retain an electronic copy of communications between company and client until matters discussed have been resolved. Details relating to health matters (such as scanned health screening questionnaire, updates from you on your health concerns) may be printed and attached to your paper-based treatment record (see below) or retained within the company email account. We have a duty to keep health records for a period of 8 years.

Mindbodyonline: Plus Health Company use an online booking system called mindbodyonline to manage bookings for all company services. This program is operated from the United States of America (USA) and where the servers and back up servers are located. In order to comply with GDPR, mindbodyonline have reached 'Privacy Shield' status, which is required by law when holding data outside of the European Union (EU). This certification demonstrates their compliance and commitment to safe handling of data and privacy.

When scheduling a booking for any of our services, we will ask for the following information: full name, email address, telephone number (mobile preferable). This will enable us to create an account for you within the system, contact you via email, get in touch should there be any changes to your booking and to send updates as/when required. You will be able to view your schedule and account information under your individual login.

We will also hold brief, relevant medical information within this program which will ensure we can work safely as a team and properly inform those involved in your care. We may also list goals/aims within the program to assist us in delivering clinical excellence and client satisfaction.

Mindbodyonline does not share data with outside parties other than those they work directly with. These may include Constant Contact (a marketing tool) and Paysafe (a merchant banking system).

Paysafe: We use Paysafe as a means of completing card payments via the mindbodyonline system. This program is directly linked to mindbodyonline but is governed separately. It is based in the Isle of Man and is ICO and GDPR compliant. For further details on their Privacy Policy, please view their website.

We are most likely to complete face to face card transactions but may also occasionally process over the telephone transactions with your permission. To process a card payment, we will require the following information: full name as it appears on your card, the 16 digit card number, expiry date, CVV (3 numbers on the back of the card) and the first line of your address and postcode. We do not automatically store any card data. However, you may wish to give your permission for us to store your card details securely in order to enhance the payment process for future occasions. We will always ask for your permission before storing this data or you may choose to do so via your individual mindbodyonline account. We do not store full card details and would only be able to identify your method of payment from the last 4 digits of your 16 digit card number.

When viewing bank statements, you will be able to easily identify your transaction with us as NBX Plus Health Co. You will also be able to track your payments and account information via your mindbodyonline account.

In order to book with us via your mindbodyonline account, you will be required to purchase your chosen service in advance using a card payment option. If you prefer not to make a card payment, we will be able to accept cash as an alternative and reserve the right to request this in advance to secure your booking(s).

Constant contact: This USA based company offers an efficient marketing tool enabling us to provide you with up to date news, company changes, promotions etc. Constant Contact are certified under EU-US Privacy Shields meaning that they comply with GDPR and safe handling of personal data. For further details, please see their privacy statement:
https://www.constantcontact.com/uk/legal/privacy-statement

We will use our existing client database from the mindbodyonline system to generate mailing lists within Constant Contact (which partners with mindbodyonline to provide a seamless process) and promise not to bombard clients with unnecessary communications. Constant Contact offers an option to opt-out of receiving future emails by clicking the SafeUnsubscribe link at the bottom of each newsletter.

Record Keeping: Plus Health Company maintain paper-based treatment records. We are required to hold accurate, up to date and detailed notes in order to comply with professional standards set by the Health and Care Professions Council: http://www.hcpc-uk.co.uk/ and our professional body, the Chartered Society of Physiotherapy: http://www.csp.org.uk/.

To use our services, you will be required to complete a self-administered health screening registration form and validated clinical outcome measure(s). This will include the following data: full name, date of birth, address, registered GP name/address, email, details about your current health status, relevant medical history, list of medications and details regarding your work and social life. It will also include a disclaimer which confirms you will keep us up to date on any health changes or changes in personal data (such as change of address or email account). We require this information to make informed decisions about how best to care for you and to comply with the professional standards listed above. Your initial consultation will explore these details more specifically.

We record each appointment visit within your personal treatment record. We list the date and time of your consultation, what you tell us (ie how you've been), record objective data such as observations, clinical tests, treatment undertaken, an analysis of our clinical effectiveness and outcomes and other factors which may contribute to your progress (such as psychosocial elements). We also document the agreed plan, when we intend to see you again and sign at the end of our treatment notes.

As part of your care, we may offer to write to your GP and/or consultant. We promise never to discuss any aspects of your care with anyone outside of the Plus Health Company team without your prior informed consent. We will be clear with you about what we wish to discuss with them and why. You will be asked to authorise the content of the letter prior to it being sent and may wish to retain a copy for your own records. We will attach a copy of any communications sent/received to your treatment record, as required to do so by our professional standards.

We will safely retain client treatment records for a period of 8 years and for children, 8 years from the time they turn 18, as required to do so in law.

We also keep a notebook to record cash payments and equipment on loan. Data recorded in these notebooks is limited to the clients name, date received/borrowed, amount paid, item loaned.

Encrypted USB: Plus Health Company may choose to hold some personal data on the company encrypted USB device. This will enable us to maintain up to date client contact details should there ever be a data loss or breach.

Social Media: Plus Health Company may choose to engage in social media (Facebook, Twitter etc). We promise never to upload any personal data onto social media without your prior informed consent. We may choose to store data you have chosen to add to our site/page yourself such as reviews, comments, photographs. Please note, by 'liking' and/or 'following' our social media content, you are consenting to others viewing your personal data as per *your* privacy options.

Website: We may ask clients to write testimonials, reviews or case studies from time to time. We will only upload content onto our website (www.plushealthcompany.co.uk) with your prior informed consent. Identifiable personal data, such as name and occupation, may be requested to add credibility to the information published.

CCTV: At our Halifax location, recordable CCTV cameras are located in thoroughfares, the upstairs studio and overlooking the Salvation Army car park to maintain client and staff safety in the event of unauthorised access, damage to property or theft. Viewing screens are located in each treatment room so members of staff can observe data in real time. Recorded data is kept for a maximum of 7 days and is then over-written with new content. CCTV footage may be reviewed occasionally by management.

CCTV is also in operation at our Huddersfield venue, Concepts Beauty. It is located on the ground floor level. For further details on how this data is managed, please contact Concepts Beauty directly.

Third Parties: We may receive personal data from third parties including insurance companies, occupational health referrals and health and rehabilitation contracts who will be subject to their own privacy policies which you may wish to review. We promise not to share any personal data with any of the above without your prior informed consent and agree to adhere to our Privacy Policy at all times.

We may also employ the services of technical support staff from time to time to assist us with Information Technology (IT) support, data breaches and to keep your data as secure as possible.

How we Keep Your Data Safe

Computer & Smart Phone Security:

- ✓ Plus Health Company install firewall and virus-checking systems on company computers and promise to keep these up to date at all times. Auto reminders are set to ensure memberships do not expire.
- ✓ Plus Health Company undertake updates on smart devices and application platforms as prompted by the companies who manage these (such as apple for iphone and ipad).
- ✓ Our operating systems are set to receive automatic updates where possible to ensure they are kept up to date.
- ✓ Staff do not share passwords other than to access a generic desktop login which does not contain any personal data.
- ✓ We change passwords every 30 days including a range of upper/lower case letters, special characters and numbers and do not share these with anyone other than the company owner.
- ✓ Staff agree to log out of their accounts after each use and promise to password-protect their devices.
- ✓ We make regular back-ups of the information stored on our computer systems and keep them in an encrypted USB device which is securely stored so if we experience a data loss of some kind, some information can be recovered.
- ✓ We promise to securely remove personal information held on computers before disposing of such by destroying the hard disk.

Email Security:

- ✓ All email content containing sensitive health information is encrypted using Egress Switch. For example, reports or treatment summaries.
- ✓ We password-protect emails containing names, addresses and details of purchases (ie receipts).
- ✓ We do not routinely encrypt or password-protect general queries but would do so upon request.
- ✓ Our email software will auto-save your email address if we have contacted you before (or you have contacted us). It may suggest your email address as we begin to type your details into the 'to' address bar. We promise to double check we are sending the correct information to the correct recipient
- ✓ We will not reveal your email address to other recipients without your prior consent. We will enter your email address in the 'BCC' (blind carbon copy) address bar when sending group emails meaning they will not be visible to anyone except us.
- ✓ We change passwords every 30 days including a range of upper/lower case letters, special characters and numbers and do not share these with anyone other than the company owner.
- ✓ Staff do not share passwords with anyone other than the company owner. Email accounts will be logged out after each use.
- ✓ We will delete unnecessary email data every 6 months.

Paper Security

- ✓ Paper-based documentation (such as treatment records) are stored securely in a lockable filing cabinet on company premises. Company premises are also kept locked and alarmed when not in use.
- ✓ Paper-based documentation will be shredded and properly disposed of following use.
- ✓ We promise not to hold your treatment record for more than 8 years (after your last visit) and for children, we will retain records for eight years after their 18 birthday or until 25 years of age.

Staff Training & Security

- ✓ Staff are familiar with our Privacy Policy and know what it expected of them. We are bound by our professional standards set by the HCPC and CSP and have a duty to protect our clients.
- ✓ Staff follow our stringent company processes to ensure personal data is kept confidential and secure.
- ✓ Staff are bound by contractual obligations which ensure a range of security measures and restrictions.
- ✓ We change passwords every 30 days including a range of upper/lower case letters, special characters and numbers and do not share these with anyone other than the company owner.
- ✓ Staff do not share passwords with anyone other than the company owner. Email accounts will be logged out after each use.
- ✓ Staff are only permitted to access and use personal data required to successfully undertake their role.
- ✓ Other than the company email address (hello@plushealthcompany.co.uk), staff email accounts are only used for internal communications. Staff know not to open spam, subscribe to mailings or accounts other than those used directly for business purposes.
- ✓ Staff are routinely screened for DBS checks and are duty bound to report any misgivings or law breaking.
- ✓ Your personal data will be routinely shared with members of staff to ensure you receive the best possible treatment and care. You may, however, which to object to this and have a right to do so. In this event, we will require clarification in writing, addressed to the data controller, to confirm how you wish to manage your personal data and state the reasons why. We will

then discuss the impact of this with you which may have an impact on our ability to provide certain aspects of treatment or care.
- ✓ Management undertake periodic checks to ensure that the organisation's security measures remain appropriate and up to date.

Physical security

Personal data is kept in our Halifax premises and the company owners home office. Both venues are well maintained and kept secure with the addition of locks, alarms, security lighting and CCTV. We also control access to our premises by limiting the number of keyholders to zones we hold personal data, do not leave personal data unattended at any time, supervise visitors as/when required and have a procedure for disposing of confidential waste.

Managing a Data Breach

In the event of a data breach, we promise we will endeavour to respond swiftly and effectively. We promise to adhere to the following process:

1. Containment and Recovery – every attempt will be made to contain the data breach and to recover any breached data. We will liaise immediately with the source of the data breach, confirm what data has been compromised and employ the support of a security specialist.
2. Assessing the Risks – we will assess the potential adverse consequences for individual(s) and evaluate how serious or substantial these are.
3. Notification of Breaches – we promise to inform people involved in an information security breach swiftly. We will notify you, the ICO (Information Commissions Office), other third parties (such as the police, banks or our partners) as necessary.
4. Evaluation and Response – we promise to investigate the cause(s) of the breach and also evaluate the effectiveness of our response to it. If necessary, we will subsequently update our policies and procedures accordingly.

Damage to Data: Where notes are damaged, such as by a fire or flood, we will attempt to restore/repair original records as far as is possible. The original record (or aspects of it) will be retained as far as is practicable.

Your Rights

The Data Protection Act states that individuals have:

- ✓ a right of access to a copy of the information comprised in their personal data;
- ✓ a right to object to processing that is likely to cause or is causing damage or distress;
- ✓ a right to prevent processing for direct marketing;
- ✓ a right to object to decisions being taken by automated means;
- ✓ a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- ✓ a right to claim compensation for damages caused by a breach of the Act.

Subject Access Request

If you wish to access the data we hold on you, we will require a request in writing addressed to the data controller (company owner). We will charge a fee of £50 and will require payment prior to the access of such data. We promise to share your day within 40 calendar days following receipt of your letter, as stipulated by law.

The Right to be Forgotten

We will respect your wish to be removed from databases, marketing lists and other methods of communication. Rather than deleting your data, we will 'inactivate' or 'suppress' it. This means we will be able to ensure your details are not re-added to the database at a later date, unless your permission for this is given. If you wish to be removed from company communications, please write to us and we will confirm this with you once actioned.

Deleting Data

Whilst you have a right to request data be deleted, we may be limited in law to do so. In this event, please write to the data controller specifying which data you wish to be removed and why. We will review this in a timely manner and discuss the outcome of this request with you directly

Obtaining Consent

One of the conditions for processing is that you, the client, have consented to your personal data being collected and used in the manner and for the purposes in question. As health professionals, we are clear on the need for consent in relation to health information, assessment and treatment. We follow recommendations set in the CSP's guidance entitled 'Consent and Physiotherapy Practice', a copy of which can be given to you upon request. As a company, it is important to us that we treat you fairly. We promise to give you the information you need and ask for in order to give your informed consent and we promise to respect your right to withdraw your consent at any time.

Making a Complaint

Whilst we will make every effort to ensure you receive a quality service from us, we appreciate there may be times when we fall short. In this event, we would urge you to report your complaint directly to the company owner/data controller who will hopefully be able to resolve your concern/issue.

If we are unable to resolve your complaint, you may wish to escalate it onwards to a supervisory authority. All physiotherapy staff are members of the HCPC, our regulatory professional body and each hold professional memberships with the CSP. The ICO would handle any complaints regarding misuse of personal data.

Updating your Data

It is important we maintain accurate, up to date details about your personal data. We encourage clients to inform us about any changes relevant in this regard. You may, however, wish to update your own personal data within the mindbodyonline system too. Once you have created an account, you will be able to modify and edit your profile and see what information is stored in the mindbodyonline program. You can opt out of receiving notifications (ie auto emails) through the mindbodyonline site too.

Changes to our Privacy Policy

We may make changes to our Privacy Policy from time to time. Updated versions will be circulated to you and available to read on our website.

Registered Company Details:

Plus Health Company Limited is a limited company registered in England and Wales.
Registration number: 10581806
Registered Office: The Studio Rooms, 11 St James Street, Halifax, HX1 5SU.
Company Owner and Data Controller: Jen Redfern