smartclinic

DATA POLICY 2023

Definitions

'Smart Clinic', 'Smart Clinic', 'Smart Clinic UK', or any references to 'us', 'we' and 'our' – refers to Smart Clinic Limited

Purpose and scope

The purpose of this document is to identify any data processing activity within the Smart Clinic, and ensure that it's being processed legally, fairly, ethically, and in line with all appropriate regulatory bodies.

At the Smart Clinic we aim to maintain adequate occupational health and wellbeing clinical records, in a way that protects the confidentiality of all our data subjects, namely our internal employees, our clients and their employees. This document should provide all the information required to those unsure about our data processing activity, or who have concerns about their privacy and confidentiality when engaging with us.

This policy is an open document, and will be made available to all employees, clients, prospective clients, or employees of our clients.

The law and regulation

We're registered in England, part of the United Kingdom, and fall under UK law. We also employ a range of different clinicians, who are bound by their individual regulatory bodies.

For the purpose of this document, we'll identify some of the core law and regulation relating to data protection.

General Data Protection Regulation (GDPR)

The GDPR is our 'holy grail' of data protection regulation. It helps to protect data subjects with the processing of their personal data, and imposes rules relating to the free movement of personal data. It protects the fundamental rights and freedoms of individuals and their personal data.

This document details exactly which factors of the GPDR are relevant to us, and how we address them.

Data Protection Act 2018

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Human Rights Act 1998

The Human Rights Act is a piece of legislation also applicable to us and our handling of data.

NMC Code

Our nursing staff are all registered with the NMC and therefore are bound by the various aspects of the NMC code of conduct.

GMC

Our doctors are all registered with the GMC, and therefore are bound by the various aspects of the GMC code of conduct.

BACP

Our counsellors are all registered with the BACP, and therefore are bound by the various aspects of the BACP code of conduct.

CSP

Our physiotherapists are all registered with the CSP, and therefore are bound by the various aspects of the CSP code of conduct.

Our philosophy and good practice

In addition to the law and regulation that we adhere to, we also have our own set of internal guidelines which we feel contribute towards an ethical approach to our work.

We have four cultural principles, which apply to all staff and form part of their induction and training. These are:

Straight talking

This is our most relevant principle to data protection. Staff are trained to be honest, open and direct. We'll never be deceptive with our information or our purposes, and do our best to keep all parties informed in a way that offers complete clarity. We make all our information as easy to understand as possible, avoiding complicated medical jargon, and where appropriate always give a full and frank answer to any questions we may be asked.

Kind

We believe that being kind goes a long way towards providing an ethical and supportive service. Often, being straight talking is the kindest approach, and we'll always be as empathetic and supportive as is appropriate for the situation.

In the context of data protection, kindness means not being deceptive about our use of data, processing it in a way that is detrimental to the health and wellbeing of the data subject, unnecessarily withholding facts or information, or making promises that we cannot keep.

We take consent very seriously, not just in the interest of data protection, but in the interest of being fair and kind to our clients. Unless falling under one of the criteria for making a deliberate data breach (see later sections), we'll never act without the explicit informed consent of our clients.

We don't believe in taking sides, or working towards any hidden agenda.

Proud

Employees and clients are encouraged to be proud of themselves and what they do. We'll never ask staff or clients to do something that they have a rightful cause to be uncomfortable with, or that they feel is unethical.

Pro-active

We often think the fairest and most beneficial action to take is a pro-active one. Employees and clients are encouraged to manage situations proactively, and that includes all matters relating to data protection. Staff are trained on various good practice techniques, such as data minimization, pseudonymization, subject access requests, right to erasure and consent, and will take a pro-active approach towards tackling these.

Principles of processing personal data (GDPR Art.5)

We will process personal data lawfully, fairly and in a transparent manner. We only collect the necessary data for the explicit purpose of the given processing activity, limiting data only to what is necessary (data minimization).

We take all reasonable steps to ensure that personal data is accurate, and where data is held inaccurately this is rectified immediately. This is done in two ways; firstly, we have an administration

team who review client files regularly, checking and cross-referencing data; secondly, all clients have access to an online client area where they themselves can edit much of the data we hold on record.

We also take all reasonable measures to ensure the utmost security of the data. Please see later information security section for more details.

Under Art.9 of the GDPR, much of the data we process is special category data, justified by Art.9 (2)(a) and (2)(b).

We recognize the following rights of the data subject (GDPR Art.12-23):

1. The right to transparent information and clear communication surrounding the processing of data (see later section)
2. When data has been supplied by the data subject the right to know specific information before data is processed, including details about the processor, the data controller, the purpose for processing, the legal basis for processing and the intended recipients
3. When data has not been supplied by the data subject the right to know specific information before data is processed, including details about the processor, the data controller, the purpose for processing, the legal basis for processing and the intended recipients – applicable both when the data has been obtained by the data subject or otherwise
4. The right to access their personal data, free of charge, and further information such as the purpose of the processing, the categories of personal data, the recipients, the period the data will be stored for, the existence of the right to erasure or rectification, how to make a complaint, the source of the data, and any automated decision making (see later section)
5. The right to rectify any incorrect personal data
6. The right to be forgotten, meaning an erasure or pseudonymization of personal data
7. The right to restrict the processing of personal data
8. The right to notification if data of any rectification or erasure of personal data or restriction of processing. to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.
9. The right to data portability
10. The right to object to the processing of data
11. The right to object to automated decision making and profiling

Data accessibility and subject data requests

We follow the ICO code of practice on data accessibility, and the GDPR Art.15.

All data subject requests will be handled by our client support team, and will be signed off by our Data Protection Officer. This will be a final check to ensure that all information has been provided and specific queries have been answered.

There will be no charge for data subject requests in the first instance, but for any further copies or unreasonable requests we shall charge an administrative fee of £20 per hour to collect the information.

All data will be provided in commonly used electronic formats including (but not limited to) .doc, .docx, .pdf, .jpeg, .xls, .msg files. These will be hosted on our server, and a link to download them will be provided to the data subject, with the necessary security validation and encryption. The data will

be available to download by the data subject for a period of no longer than seven days, after which any further requests will be constitute 'further copies' and will be chargeable at the above rate.

To make a data subject request, clients can log into their client area and use the 'subject data request' form. Alternatively, much of the information stored on a client will be accessible in the form of downloads already, should they choose to access it immediately.

If you no longer have access to our client area, because your package has elapsed or you have changed employer, you can request our subject data request form by emailing DPO@smartclinic.com – please note if you have an active client area, you will be directed to that in order to make your request.

We strive to respond to confirm data subject requests within seven calendar days, and to provide the data within 30 calendar days. This doesn't include any delay caused by the data subject for reasons such as needing clarification, or validating identification.

Right to erasure (right to be forgotten)

For our guidance on the right to erasure we follow GDPR Art.17.

All data subjects have the right to have their personal data concerning the individual erased, when one of the following applies:

- The data is no longer necessary for the purpose it was collected for
- The data subject withdraws consent on which the processing is based
- The data has been processed unlawfully
- There is a legal basis for the erasure of the data
- The personal data have been collected in relation to the offer of information society services referred to in Art.8(1)
- The data subject objects to the processing pursuant to Art.21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Art.21(2)

Where any of the requested data has been made public, we'll take all reasonable steps to inform the data subject or the person making the request where this public data can be found.

There may be instances in which we can't comply with a request for erasure. For instance:

- Exercising the right of freedom of expression and information
- compliance with a legal obligation
- If part of a task being carried our in the public interest, including but not limited to public health, scientific research or statistical purposes
- For the establishment, exercise or defence of legal claims

To make a data erasure request, clients can log into their client area and use the 'data erasure request' form.

If you no longer have access to our client area, because your package has elapsed or you have changed employer, you can request our data erasure form by emailing DPO@smartclinic.com – please note if you have an active client area, you may be directed to that in order to make your request.

Data retention schedule / record of processing activities

GDPR (Art 5 (1)(e)) forbids data to be kept in a form which allows for the identification of a data subject for longer than is necessary for the purposes for which the data is being processed.

Our schedule for retaining and erasing data is as follows (correct at 25th May 2018):

Pale turquoise rows represent special category data

Business function	Purpose of processing	Categories of individuals	Categories of personal data	Categories of recipients	Retention schedule (if possible)	Article 6 lawful basis for processing personal data
Finance	Payroll	Employees	Contact details	HMRC	5 years post-employment	Article 6(1)(c) - legal obligation
Finance	Payroll	Employees	Bank details	HMRC	3 years post-employment	Article 6(1)(c) - legal obligation
Finance	Payroll	Employees	Pension details	HMRC	75 years post-employment	Article 6(1)(c) - legal obligation
Finance	Payroll	Employees	Tax details	HMRC	6 years post-employment	Article 6(1)(c) - legal obligation
Finance	Invoicing	Contractors	Bank details	N/A	6 years post-employment	Article 6(1)(b) – contract Article 6(1)(c) - legal obligation
Human Resources	Personnel file	Employees	Contact details	N/A	6 years post-employment	Article 6(1)(b) – contract Article 6(1)(c) - legal obligation
Human Resources	Personnel file	Employees	Pay details	N/A	6 years post-employment	Article 6(1)(b) – contract
Human Resources	Personnel file	Employees	Annual leave details	N/A	6 years post-employment	Article 6(1)(b) – contract
Human Resources	Personnel file	Employees	Sick leave details	N/A	6 years post-employment	Article 6(1)(b) – contract
Human Resources	Personnel file	Employees	Performance details	N/A	6 years post-employment	Article 6(1)(b) - contract
Human Resources	Recruitment	Successful candidates	Contact details	Referee	6 years post-employment	Article 6(1)(a) - consent Article 6(1)(b) - contract
Human Resources	Recruitment	Successful candidates	Qualifications	N/A	6 years post-employment	Article 6(1)(b) - contract

Human Resources	Recruitment	Successful candidates	Employment history	N/A	6 years post-employment	Article 6(1)(a) - consent Article 6(1)(b) – contract
Human Resources	Recruitment	Unsuccessful candidates	Contact details	N/A	6 months post-campaign	Article 6(1)(b) - contract
Human Resources	Recruitment	Unsuccessful candidates	Employment history	N/A	6 months post-campaign	Article 6(1)(b) - contract
Clinical team	Occupational health assessments	Employees of our clients / sub-clients	Contact details	Designated client / sub-client contacts	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(b) – contract
Clinical team	Occupational health assessments	Employees of our clients / sub-clients	GP details	Designated client / sub-client contacts	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(d) – vital interests
Clinical team	Occupational health assessments	Employees of our clients / sub-clients	Medical records / referral details	Designated client / sub-client contacts	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine
Clinical team	Occupational health assessments	Employees of our clients / sub-clients	Medical records / internal notes / audio and video recordings	Designated client / sub-client contacts	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine
Clinical team	Occupational health assessments	Employees of our clients / sub-clients	Medical records / external reports	Designated client / sub-client contacts	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine
Clinical team	Pre-placement assessments	Employees of our clients / sub-clients	Contact details	Designated client / sub-client contacts	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(b) – contract
Clinical team	Pre-placement assessments	Employees of our clients / sub-clients	GP details	Designated client / sub-client contacts	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(d) – vital interests
Clinical team	Pre-placement assessments	Employees of our clients / sub-clients	Medical records / referral details	Designated client / sub-client contacts	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(d) – vital interests
Clinical team	Pre-placement assessments	Employees of our clients / sub-clients	Medical records / internal notes / audio and video recordings	Designated client / sub-client contacts	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine
Clinical team	Pre-placement assessments	Employees of our clients / sub-clients	Medical records / external reports	Designated client / sub-client contacts	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine

Clinical team	Talking therapy	Employees of our clients / sub-clients	Contact details	N/A	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(b) – contract
Clinical team	Talking therapy	Employees of our clients / sub-clients	GP details	N/A	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(d) – vital interests
Clinical team	Talking therapy	Employees of our clients / sub-clients	Medical records / referral details	N/A	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine
Clinical team	Talking therapy	Employees of our clients / sub-clients	Medical records / internal notes / audio and video recordings	N/A	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine
Clinical team	Talking therapy	Employees of our clients / sub-clients	Medical records / external reports	N/A	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine
Clinical team	Physiotherapy	Employees of our clients / sub-clients	Contact details	N/A	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(b) – contract
Clinical team	Physiotherapy	Employees of our clients / sub-clients	Medical records / referral details	N/A	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine
Clinical team	Physiotherapy	Employees of our clients / sub-clients	Medical records / internal notes / audio and video recordings	N/A	6 years post-contract termination	Article 9(2)(a) – consent Article 9(2)(b) – employment Article 9(2)(c) – vital interests Article 9(2)(h) – occupational medicine
Clinical team	EAP	Employees of our clients / sub-clients	Contact details	N/A	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(b) – contract
Clinical team	Virtual GP	Employees of our clients / sub-clients	Contact details	N/A	6 years post-contract termination	Article 6(1)(a) – consent Article 6(1)(b) – contract Article 6(1)(f)
Clinical team	Health checks	Employees of our clients / sub-clients	Medical records / internal notes	N/A	6 years post-contract termination	Article 6(1)(b) – contract Article 6(1)(a) – consent Article 6(1)(c) - legal obligation Article 9 (2)(b) Employment Article 9 (2c) vital interests Article 9(2)(f) legal defence

						Article 9(2)(h) occupational medicine
Clinical team	Health checks	Employees of our clients / sub-clients	Medical records / external reports	N/A	6 years post-contract termination	Article 6(1)(b) – contract Article 6(1)(a) – consent Article 6(1)(c) - legal obligation Article 9 (2)(b) Employment Article 9 (2c) vital interests Article 9(2)(f) legal defence Article 9(2)(h) occupational medicine
Clinical team	Telephone calls	All	All	All	6 years post-contract termination	Article 6(1)(b) – contract Article 6(1)(a) – consent Article 6(1)(c) - legal obligation Article 9 (2)(b) Employment Article 9 (2c) vital interests Article 9(2)(f) legal defence Article 9(2)(h) occupational medicine
Clinical team	Health surveillance records	Employees of our clients / sub-clients	Medical records / internal notes	N/A	40 years post-contract termination	Article 6(1)(b) – contract Article 6(1)(a) – consent Article 6(1)(c) - legal obligation Article 9 (2)(b) Employment Article 9 (2c) vital interests Article 9(2)(f) legal defence Article 9(2)(h) occupational medicine
Marketing	Email marketing	Clients, sub-clients, employees, potential clients	Contact details	N/A	1 year after campaign	Article 6(1)(f) – legitimate interests See appendix 1

Consent

Consent is fundamental to our processing of data.

We take the following steps to demonstrate that consent has been given to process the specific data:

- Telephone calls where verbal consent has been given are recorded and stored
- Records of written and signed consent are stored for each case or…
- Records, time stamps and IP addresses for digital consent are stored for each case
- Clients are regularly reminded of their right to withdraw consent at any given time
- All consent forms or digital versions of consent offer clear, specific detail on exactly what is being consented to (often to conduct an appointment with us, engage in therapy, or release information)

To ensure consent is kept as specific and clear as possible, we have a number of different consent forms and digital consent wording. For our most up to date standardized consent wording for any given service, please make a request to hello@smartclinic.com and we'll be happy to help.

If at any stage we suspect that the data subject has given consent under coercion or duress, and the consent is not freely given, we reserve the right to halt the data processing and seek clarification or refuse to process the data any further.

Clear communication and language

There are a number of references in the GDPR to clear, easy to understand use of language. This is particularly relevant to us at the Smart Clinic, not least when it comes to consent, so we've decided to feature it as a section in our data policy as well as our brand guidelines.

We adopt an informal, professional and direct tone of voice. Staff are encouraged to write how they would speak, avoiding long sentences and paragraphs. They're trained not to use jargon, or overly complicated phrases.

We also break up the information that we request or offer into 'chunks' with clearly labelled sections. This makes it easier to understand and digest and becomes less overwhelming. It also helps with referring to information at a later date.

We believe in using this approach because using simple and clear language ensures that everyone who engages with us fully understands the nature of the data processing and is able to give informed consent. We strive to offer appropriate, regular and clear information, and are always reviewing our processes to better achieve this.

If you have any suggestions on how we can be clearer with our information, please email hello@smartclinic.com.

Processing data without consent

Although consent is not the only justification for processing data (normal or special category) it should be taken for most of our processing activities, not least to keep the data subject informed. However there are instances whereby it is lawful and we're duty bound to break protocol, and process data without consent, as described in GDPR Art.6 and GDPR Art.9 For instance:

- Processing is necessary for compliance with a legal obligation e.g. where a court order has been obtained by the police to search medical records
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person e.g. where an individual's life is at risk
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child
- processing is necessary for carrying out the obligations in the field of employment e.g. information for decisions on disciplinaries, salary payments, dismissal and redundancy
- processing is necessary for the establishment, exercise or defense of legal claims

Accidental breaches of data

In the unlikely and rare event that a data breach has occurred:

- If the breach is likely to result in a risk to the rights and freedoms of the data subject, inform the relevant supervisory authority within 72 hours.
- Document the data breach, the effects, and any remedial actions taken
- If the breach is likely to result in a high risk to the rights and freedoms of the data subject, we'll communicate the personal data breach to the data subject without undue delay. This will be clear and in plain language, as per the above section on clear communication. The exceptions to this would be
    - If the breached data is unintelligible to any person not authorized to access it (such as encryption)
    - There is no longer a high risk to the rights and freedoms of the data subject
    - It would take disproportionate effort

GDPR Art. 77-84 details the rights of the data subject, our liability, and any penalties that may be imposed on us as a result.

In summary the data subject has the right to:

- Lodge a complaint with a supervisory authority, without prejudice
- An effective judicial remedy against a supervisory authority
- An effective judicial remedy against us
- Representation
- Compensation and liability, proportionate to the material or non-material damage as a result

Marketing opt in policy

This section relates to direct (text, email, telesales and postal) marketing and social media. We use the GDPR and Privacy and Electronics Communications Regulation (PECR) to steer our data processing for the use of marketing.

Our marketing lists are compiled fairly and accurately to reflect the wishes of customers and prospective customers.

The Direct Marketing Association write:

"When dealing with employees of corporates – that is, limited companies, LLPs, partnerships in Scotland and government departments – the rules for telephone and direct mail are the same, opt-out. When emailing or texting, you do not need the prior consent/opt-in from the individual. You can therefore send them a marketing email/text as long as you provide an easy way to opt out of future communications from you."

In Art.6 of the GDPR, one of the conditions (F) for lawful processing reads

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

In Recital 47 of the GDPR it reads:

"The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

Therefore, we feel that B2B email marketing, postal marketing, telesales and text marketing are legitimate interests, and fall within the lawfulness of processing data, and as such are acceptable.

Please see appendix 1 for a legitimate interest assessment where we've determined this in more detail.

Information security

This section details how our IT systems are developed, built and maintained to comply with GDPR and provide maximum protection to the data subjects.

Local storage

All data is kept behind a fully managed, up to date dedicated firewall, standard ports are masked by being changed to non-standard numbers. Intrusion detection systems are in-place to monitor all data flowing in and out of the network.

All data stored on the local network is encrypted with a 2048bit key based encryption algorithm, the passphrase for decryption is kept with the private key in a secure location away from the server and not in the network.

No data is transferred out of the network, files stored on the network are only accessible from within the network with the use of a personal username and password to log the access to the stored information.

Remote server

All files stored on the remote server are within folders that allow access only to the web servers user. Read and write access is restricted via permissions to prevent the leakage of files and the unauthorised access to outsiders. All data transferred to and from the server is secure with SSL which is automatically renewed to ensure continually security.

Databases and password management

All databases have unique usernames and passwords, the passwords for the databases are create without the use of words and are not familiar to anything linked to a member of staff. They are 8 characters or longer and must include uppercase and lowercase letters, numbers and special characters. All passwords are refreshed every 3 months and are not allowed to use previous passwords.

Users are asked to create their own passwords that must be at least 8 characters long. Every use has a unique ID as well as a privilege level that grants access to the system, they are also blocked from accessing the system outside of working hours.

Users accounts are disabled as soon as it is known they are not returning to their employment.

Backups

Both website documents and remote databases are backed up every night. Each night a tar is created of that day's files and placed into a daily folder. On Monday of each week a weekly tar is created and on the first of each month a monthly tar is created. A total of 7 daily, 4 weekly and 12 monthlies are kept for the first year. Following that a yearly tar will be created.

Backups of local servers are created when a major update or reconfiguration is created, as these servers are run through a virtual environment the backups are complete operating systems allowing for very fast recovery and deployment.

Daily and weekly backups are stored locally on the server that is creating the backups, this server is encrypted allowing for secure local storage. The monthly tar backups are encrypted on the local server before being securely transferred to the local NAS.

All backups performed are replicated in two different physical locations. Each location contains an identical copy of the data being backed up by the company at all times.

Website data

Security: SSL Certs, Restricted folder permissions, .htaccess restrictions, SFTP connections for access to public_html (unique accounts per developer), public/private SSH keys for server access.

Hosted on dedicated servers supplied by Heart Internet Limited

Password encryption

In our Smart Clinic Web application, ensuring the security of user passwords is paramount. To achieve this, we employ the bcrypt hashing algorithm for password storage. Here is some useful information on how the hashing Algorithm works.

Storing plaintext passwords in the database is risky, as it leaves them vulnerable to exploitation in case of a breach. By using password hashing, we convert passwords into irreversible hashes, significantly enhancing security.

Bcrypt is a widely recognized and slow cryptographic algorithm. Its deliberately slow nature makes brute-force attacks practically infeasible, even with access to hashed passwords.

Bcrypt's strength lies in its "cost factor." Setting a higher cost factor increases the time required to generate a hash, enhancing security. Our application utilizes a cost factor of 12, a recommended balance between security and performance.

When users create or update passwords:

a. Bcrypt generates a unique, cryptographic salt for each password.

b. The salt combines with the plaintext password and undergoes a key derivation function, creating the irreversible password hash.

During login attempts, we employ PHP password_verify() function to compare entered passwords with stored hashes. The function automatically handles salt extraction and hash comparison.

With bcrypt hashing, we prioritize the protection of user passwords in our application. By employing this slow and resilient algorithm with a well-chosen cost factor, we fortify our security measures to safeguard user data effectively.

Feedback / complaints procedure

At Smart Clinic we do our best to provide a high quality service and live up to expectations as much as possible. However we recognize that we aren’t perfect; mistakes can happen and we can make improvements in many areas of the business.

We would welcome all feedback, good or bad, and would encourage this to be submitted to us informally or formally.

Informal feedback

All customers are welcome to document their feedback, queries or concerns to hello@smartclinic.com. Whilst this would be treated as informal feedback, we'll still endeavor to investigate the issue and provide a full and frank response within three working days. If we can't do this, we'll inform you of the delay and let you know when you can expect to receive a response to us.

We'd encourage all customers to use this method in the first instance, as it's the most time efficient means for both parties and means that you will get the fastest possible response.

Alternatively, we have a feedback form on Survey Monkey (https://www.surveymonkey.co.uk/r/P2G83YC) – for every completion of this form we donate £1 to Medecins Sans Frontieres. Comments can be left anonymously, and all feedback is reviewed and considered, however you may not receive a response.

Formal feedback form

If you feel your informal feedback hasn't received the response you would like, or would prefer to formalize your feedback immediately, please contact hello@smartclinic.com and request our Formal Feedback Form. This will detail any of our governing bodies for our various business activity, should you wish your feedback to be received by an external third party.

Your formal feedback will be treated with the utmost concern, and we may need to launch an internal investigation into the matter. This will be conducted by an Occupational Health Manager, and signed off by a company director, or conducted by the company director and signed off by an Occupational Health Manager. This will include a synopsis of events, a suggested resolution, and any further actions that should be taken as a result of the feedback.

Any data breaches, or data protection issues, will follow the formal feedback process. We'll inform the data subject in line with Art. 33 of the GDPR.

Refusing a case

The team at Smart Clinic reserve the right to refuse to process data or handle a case, based on ethical, clinical or data protection grounds.

The decision not to process data or handle a referral will be made only by the occupational health manager, or a director, and in such an instance a client coordinator will make every effort to communicate this effectively to the client.

Examples include, but are not limited to:

- Ethical – if we feel that it would be unethical to process data, for instance a member of staff is clearly distressed.
- Clinical – there are times when it wouldn't be clinically appropriate to process a case, for instance if a member of staff isn't well enough to proceed with a referral, or by doing so we could be putting the member of staff at increased risk.
- Data protection – if we have any concerns over the lawfulness of processing data, for instance if we feel that consent hasn't been appropriately and freely given.

Employee sanctions

We do everything we can to prevent data breaches, or any misuse of personal data. However we recognize that humans (us and our staff included) are fallible, and mistakes can happen. We mitigate this by systemizing as much as possible, however this isn't always possible or appropriate.

We take a common-sense approach to sanctioning employees for data breaches, also considering our internal HR guidelines. Employee sanctions range from an informal conversation about our standards, through to dismissal due to gross misconduct.

Importantly, we also learn from our mistakes. If an employee makes a mistake, they alone may not be responsible, so we always take action to prevent a similar thing from happening in the future.

Transfer of data – from a third party to us

Where possible, we encourage client organisations to retain the data for their employee's themselves, to avoid the need for a transfer of data when changing contract. As we do not undertake statutory health surveillance work, there should be little need to obtain any records that have not previously been released to your organisation with the consent of an employee.

On the commencement of a service there may be a requirement for Smart Clinic to take receipt of personal and/or special data held previously on behalf of your organisation, relating to current or former employees. The data transferred should be under the responsibility of a clinician who has the overriding responsibility for the delivery of occupational health services for that client. A clinician should be a qualified and hold a valid registration with either: General Medical Council, Nursing Midwifery Council or the Health Care Professions Council. On receipt of the details of the clinician responsible, we will also provide the details of a suitably qualified clinician from the Smart Clinic who will receive the data, and provide confirmation of receipt in writing.

Before the transfer of data takes place your organisation may wish to consult with any affected employees or make employees aware that there is a new occupational health service taking over the services. There is no longer a requirement to obtain the consent from every Data Subject the Data Protection Act (2018) permits the processing of the data for the purposes of occupational medicine.

The overriding responsibility is towards protecting the data of those whom the records belong to, and therefore we will make every effort to ensure the process is handled promptly, securely and by a suitably qualified professional. Ultimately, it is the outgoing provider's responsibility to transfer the data to us securely, effectively and in an accessible format. It is the newly appointed provider's responsibility, on receipt of the data, to accept it, store it and process it securely.

Formats we can accept or send data in include digitally encrypted data files sent via an online sharing portal or USB stick posted. We will do our best to use any other methods that fit with the other provider wherever possible, but cannot guarantee this.

An index of the files being transferred listing the names or identifiers of each Data Subject should be sent by the transferring provider to the receiving provider. There should be consignment documentation confirming the transfer of the number of files and confirming the index is accurate and all files have been received. Confirmation of receipt of the data should be sent back to the transferring provider.

We would discourage using physical records for security reasons. However where the data is physical i.e. paper and being transferred it should be securely packed with each parcel referenced and indexed to identify the total number of parcels in the consignment. An index of the files being transferred listing the names or identifiers of each Data Subject should be sent by the transferring

provider to the receiving provider. There should be consignment documentation confirming the transfer of the number of files and confirming the index is accurate and all files have been received. Confirmation of receipt of the data should be sent back to the transferring provider.

The above only includes records relating to occupational health cases, and does not include any of our wellbeing services including (but not limited to) counselling, physiotherapy and virtual GP services.

Transfer of data – from us to a third-party provider, or if you cease trading

As above we encourage client organisations to retain the data for their employee's themselves, to avoid the need for a transfer of data when changing contract. As we do not undertake statutory health surveillance work, there should be little need to obtain any records that have not previously been released to your organisation with the consent of an employee.

If an organisation chooses to cease using Smart Clinic services for any reason, or if the Smart Clinic cease trading and are unable to fulfil our obligations, any copies of occupational health reports where an employee has already consented to the release of the report can be found and downloaded directly from your client area. Any further records (such as clinical notes) will continue to be stored in line with the retention schedule listed in this policy.

If the services of a third party occupational health provider are engaged by you, and there is a need to transfer records for any reason not considered above, we will emulate the process noted in the above section (Transfer of data – from a third party to us).

Data protection officer(s)

Currently, the data protection officer for Smart Clinic is:

Harry Cramer

Director

Appendix 1 – Legitimate interest assessment

Direct marketing campaigns

Identification of the Legitimate Interest

	Question	Response
1	**What is the purpose of the processing operation?**	To provide our target customer base, Schools and organisations in England and Wales, with marketing and product information relating to our occupational health and wellbeing services.
2	**Is the processing necessary to meet on or more specific organisational objectives?**	It is necessary to spread awareness of our product, the benefits it can provide and how to access our services.
3	**Is the processing necessary to meet one or more specific objectives of any third party?**	Third parties that would also benefit from the marketing are our insurance clients, Absence Protection Ltd, Teacher Absence Ltd, Harrington Bates (Risk Management) Ltd and School Shield Ltd.

4	**Does the GDPR, ePrivacy Regulation/PECR or other national legislation specifically identify the processing activity as being a legitimate activity, subject to the completion of a balancing test and positive outcome?**	Direct marketing is identified as a legitimate interest within the GDPR provided that the interests of both parties are balanced, and the data subject's rights are not infringed upon.

The Necessity Test

	Question	Response
1	**Why is the processing activity important to the Controller?**	The activity is important to spread awareness of the product and by doing so, increase quotations and sales of the product. It is necessary to grow and expand the business.
2	**Why is the processing activity important to other parties the data may be disclosed to, if applicable?**	The only time the data will be disclosed to other parties is if a contract is being pursued, in which case legitimate interest would no longer be the primary lawful reason for processing and this would change to taking steps to enter into a contract.
3	**Is there another way of achieving the objective?**	There is no other way to reach the levels of exposure we require to grow without directly marketing to the target audience. Postal campaigns would be far too costly and not reasonable to process.

The Balancing Test

	Question	Response
1	**Would the individual expect the processing activity to take place?**	Direct contact via email is only made to the individuals personalised work email address therefore it stands to reason that they would expect to receive emails of this nature marketing products aimed towards their employer. Occupational health is either a requirement for the employer of the individual or at least a legitimate interest of theirs to explore.
2	**Does the processing add value to a product or service that the individual uses?**	The processing makes them aware of statistics, trends and previously unknown information that may help influence their decision to engage with our products/services.
3	**Is the processing likely to negatively impact the individual's rights?**	We do not consider the processing to negatively impact their rights as they are provided with the reasoning for being contacted within each email and have a clear and simple process for opting out or objecting to the processing.
4	**Is the processing likely to result in unwarranted harm or distress to the individual?**	No – see above.

5	**Would there be a prejudice to the Data Controller if the processing does not happen?**	The controller would be placed in a disadvantageous market position if it were unable to engage in the marketing activity as we would not be able to compete with the similar strategies implemented by our direct competitors.
6	**Would there be a prejudice to the Third Party if processing does not happen?**	As above.
7	**Is the processing in the interest of the individual whose personal data it relates to?**	Yes, not from a personal level but certainly from a professional level. As the email addresses in question are work emails, it stands to reason that the professional interests would be considered as a valid interest to process the data.
8	**Are the legitimate interests of the individual aligned with the party looking to rely on their legitimate interests for the processing?**	Yes, the interests of the individual's employers are aligned with our own and with the processing only involving work email addresses, these would then align with the individual.
9	**What is the connection between the individual and the organisations?**	We offer a specialised insurance product to the employer of the individual. The individuals are responsible for the business decisions of their employer.
10	**What is the nature of the data to be processed? Does data of this nature have any special protections under the GDPR?**	Only names, job title and email addresses of the individuals. The names and job titles are readily available in the public domain, so the email addresses are the main pieces of personal data to be processed. There are no special protections for this under the GDPR.
11	**Is there a two-way relationship in place between the organisation and the individual whose personal information is going to be processed? If so, how close is that relationship?**	See response to number 9.
12	**Would the processing limit or undermine the rights of the individual?**	No, opt-out is available and the scope and reason for processing is made clear in the communications.
13	**Has the personal information been obtained directly from the individual, or obtained indirectly?**	Directly through sales activity and client development. Indirectly from a central database of Schools.
14	**Is there any imbalance in who holds the power between the organisation and the individual?**	Individuals can opt-out or request a change in the contact details that we hold to nominate another individual to receive the communications so there is no imbalance.
15	**Is it likely that the individual may expect their information to be used for this purpose?**	Yes, as the primary business contact for the employer, the individual would expect to be contacted in regard to related services and products that the employer would have a legitimate interest in.
16	**Could the processing be considered intrusive or inappropriate? In particular, could it be perceived as such by the individual or in the context of the relationship?**	We do not believe this would be the case, the processing is proportional and within the expectations of the position the individual holds with their employer. A one click opt-out ensures that they can disengage from us at any time.

17	**Is a fair processing notice provided to the individual? If so, how? Are they sufficiently clear and up front regarding the purposes of the processing?**	Notice is provided for customers, previous customers or potential customers who have engaged with us by receiving quotes. It is not provided when directly marketing to new individuals we have not previously dealt with. The information relating to the process for the processing and the legitimate interests are provided within the direct marketing emails and opt-out is made clear in each communication.
18	**Can the individual, whose data is being processed, control the processing activity or object to it?**	Yes, as mentioned above the individual can either opt-out or request that the individual contact person is changed to another individual within their business.
19	**Can the scope of the processing be modified to reduce/mitigate any underlying privacy risks or harms?**	Yes, marketing campaigns can be targeted to specific individuals and if a communication is not relevant to a certain group, they will not be included. Renewal information for example would only be provided to existing customers, however, new business details could be targeted to individuals who have not previously engaged us.

Safeguards and Compensating Controls

Safeguards include a range of compensating controls or measures which may be put in place to protect the individual, or to reduce any risks or potentially negative impacts of processing. These are likely to have been identified via a Privacy Impact Assessment conducted in relation to the proposed activity. For example: data minimisation, de-identification, technical and organisational measures, privacy by design, adding extra transparency, additional layers of encryption, multi-factor authentication, retention, restricted access, opt-out options, hashing, salting and other technical security methods used to protect data.
Primary safeguards would consist of the provision of a simple opt-out system that can remove the individual from the marketing database and prevent any further unwarranted contact. The database itself is held within the processors internal systems and is backed up regularly and encrypted to help prevent unauthorised access. Communications sent to the individuals are put through multiple levels of approval prior to the communications being issued to ensure the information is relevant to the individual. Marketing communications are targeted so that only relevant information is sent to each individual.

Decision & Outcome

Outcome of Assessment:
The nature and scope of the processing is within the typical expectations of the individuals involved. They would reasonably expect marketing type communications that are relevant to their employer to be received directly to their work email addresses as the primary business contacts for their School. A simple and clear opt-out option is available within every communication and the purpose and legitimate interests being pursued are also made clear within the emails.

With the existence of these measures, we do not feel that there is a negative impact on the rights of the data subject and the legitimate interest exists on both sides of the relationship.

Provided that the information being communicated remains unobtrusive, proportionate and relevant to the individual's business interests, there is no concern that the data subject's rights are in danger.

The outcome of the legitimate interest assessment is that the direct marketing campaigns to the personalised work email addresses of individuals is within the scope of a legitimate interest as outlined within the GDPR, ePrivacy Regulations/PECR and that the processing activity can be implemented without breaching Data Protection law.