Salve Technologies Limited Data Protection Policy
with Information Governance and Security Policies

App means the Salve (mobile and web) App.

Applicable Legislation means Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). In case of discrepancy between the two, DPA shall prevail before 25th May 2018, whereas GDPR shall prevail as of 25th May 2018).

Board of Directors means Salve Board of Directors.

Data means personal data that is processed in the context of the Service, regardless of where the processing or the storage of the data takes place (terminal equipment such as personal computers, tablets or mobile phones, Salve servers, Salve leased cloud infrastructure, on our Salve premises or outside Salve premises, in electronic, printed, or any other form.

Health Data is Data in relation to an individual's health, as defined by the Applicable Legislation.

IG means Information Governance.

Policy means Salve Data Protection Policy, Information Governance (IG) Policy and Security Policy, each one of them separately or all of them together, including their Appendices.

Purpose means one or more lawful purposes of the processing of the

Data. **Salve** means Salve Technologies Limited.

Service means the Website and the App, both of them together or either of them separately.

Service User is an individual that uses the Service.

Website means the Salve patient portal, the Salve clinic portal, and the Salve website, all of them together or any of them separately.

This Policy:

- clarifies in detail the scope of the Service User's consent to use the Data; •
- regulates our processing of personal information in relation to the Service, including Health Data;
- includes the IG management framework.

This Policy has been approved by a resolution of the Board of Directors on 1 June 2017.

This Policy is based on the following documents and should in doubt always be read in compliance with them:

- Applicable Legislation

- The 2013 Caldicott Principles
- NHS Information Governance (IG) Toolkit Business Partners' requirements, Minimum Attainment Level 2
- NHS legal & security guidance for developers: https://developer.nhs.uk/library/save-legal-secure/
- HM Government Cyber Essentials Requirements.

The Data Controller

The Data Controller in relation to the Data processed in the context of the Service shall be:
Salve Technologies Limited
Unit 6, Queen's Yard, White Post Lane, London, E95EN
Rapid communication contact email: contact@salveapp.co.uk
Data Protection Officer contact: Elin Ng elin@salveapp.co.uk
Companies House reg. number: 10511483
ICO registration reference: ZA246232

Salve's status as the Data Controller in relation to the Data does not affect the status of the clinics who originally provide the data for the Service as being the data controllers for some of the same data that Salve processes in the context of the Service. Unless otherwise indicated by this Policy, Salve is processing Service Users' data based on the consent obtained directly from them at the point when they install the App or sign up for the Website.

The Purpose of Salve's Data Processing Activities

Salve is authorised as the data controller:

- to obtain Service User's personal Health Data and other personal Data from his or her medical clinic via an online communications interface, in real time or otherwise, and to process this and any additional information that the Service User will be communicating via the Service for the Purpose of managing his or her medical treatments, by him/herself and his/her medical clinic;
- to use the same Data to enhance Service Users' experience and for the maintenance of the Service;
- to pseudonymise and anonymise the same Data;
- to use the same Data in pseudonymised form for the purposes of medical treatment research, account re-activation, analytics and further development of the Service, for up to five (5) years after the end of the Service User's treatment.

For the Purpose of managing the Service User's medical treatments, the App may offer to the Service User various features such as:

- Managing medications
- Managing appointments

• Providing robust medical information

• Enabling secure messaging between the Service User and the clinical staff.

Whereas the Data is obtained from the Service User's fertility clinic, some of the data may be transmitted back to the clinic.

In most cases, Service User Data shall be pseudonymised before being used for the any other Purpose than supporting direct care by the medical clinic utilising the Service.

Anonymised Data no longer constitutes personal data because the Service User can no longer be identified, with the risk of re-identification being so low that it is deemed acceptable.

Data that we process

Service Users' Data that we process will in most cases be classified as Health Data, which constitutes a special category of sensitive personal data. Such data would typically include but is not limited to: Service User's (patient's) personal information such as name and date of birth, Service activities log, embryology, information on prescription drugs type, drug name and regimen plus notes pertaining to these types of personal information and messages exchanged between the Service User and medical professionals at his or her clinic, including metadata pertaining to such messages.

Apart from Health Data, we may process the following Data about our Service Users or other individuals that might not constitute sensitive personal data: • Other personal details such as email contact, mobile telephone number or gender

• Family, lifestyle and social circumstances

• Financial details

• Employment or education details.

Moreover, we may process other sensitive classes of our Service Users' information that may include:

• mental health details

• genetic or biometric data

• racial or ethnic origin

• religious or other beliefs of a similar nature.

Service architecture

Our Service architecture, which is Cloud-based, comprises technical and organisational measures to protect personal information and to ensure that, by default, only personal data which are necessary for each specific Purpose of the processing are processed. Accordingly, we endeavour to minimise the scope of the Data that is pulled from the clinics and stored in our Cloud to the Data that may be relevant to the Service User or our health-related research and Service analytics.

Our Service architecture may from time to time change. However, we will endeavour

to keep the same high standards of technical and organisational measures to protect privacy.

Staff access to the Data

All the existing staff are required to be aware of their IG and privacy-related obligations regarding the Data. All staff engaged in supporting any Data sharing purposes that may be required are required to understand what is lawful and what is not. All new staff are appropriately vetted / screened, trained and provided with guidelines to ensure they are aware of their obligations, data audit trails, and other monitoring procedures before they start handling the Data.

All staff are required to read this Policy and to receive annual training plus any additional training that might be required based on organisational or technological changes and/or any Data Protection Impact Assessment performed.

Sharing the Data

Health data must be kept confidential and disclosed only in the circumstances permitted by law. We shall ensure that Service Users do not have access to any other person's records without first getting that person's consent.

All purposes that require confidential personal data to be used or shared have been identified in this Policy and have a clear basis in the law.

We may disclose information that does not identify or could not reasonably be expected to lead to the identification of a Service User. If we are unsure whether information we propose to disclose could identify a person, we shall seek independent legal advice.

We may sometimes, in line with Applicable Legislation, need to share some of the Data we process with other organisations or individuals.

Cross-border transfers

It is our policy to keep the Data in the UK and/or the EU/EEA. We therefore conclude storage and processing arrangements that guarantee such data residency. Where guarantees of data residency would not be possible to obtain or would be associated with considerable difficulties, we subject every cross-border transfer of the Data to Applicable Legislation.

Access to the Data

Subject access requests are actioned by our fully trained and resourced staff, and all staff members are aware of the need to support subject access requests, and where in the organisation such requests should be directed. Subject access training shall be part of the introductory and regular staff training.

We will send the Data requested within a 40-day time frame to the Service User or another individual in relation to whom we process the Data in a commonly used electronic form.

Together with the Data, we shall also send the relevant information on: (a) the Purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with the Information Commissioner; (g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, and, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Service User.

We will charge a fee of £10 for any request received before 25th May 2018. As of that date, we will only charge a fee for the sending of an additional copy of the Data, or where the requests from the Service User are manifestly unfounded or excessive, in particular because of their repetitive character. In such cases, we might refuse to act on the request.

Termination of the processing of the Data

The Data may be anonymised at any time, and shall be pseudonymised no later than five (5) years after we have learned from the Service User or the clinic that the Service User is no longer using the fertility treatment.

The Data pertaining to a Service User will be deleted without undue delay if we receive their withdrawal of consent, and may after that only continue to be processed in anonymised form. The Service User shall have a further right to obtain from us without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the Service User shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

As of 25th May 2018, the Service User shall have the right to receive the personal data concerning him or her, which he or she has provided to Salve, in a structured, commonly used and machine-readable format, and have the right to transmit such data to another controller without hindrance.

Complaint procedures

Without prejudice to any other administrative or judicial remedy, every Service User shall have the right to lodge a complaint with any competent data protection supervisory authority, which is in the UK the Information Commissioner, if the Service User considers that the processing of personal data relating to him or her infringes Applicable Legislation.

Accessibility

When working with the clinics, we shall coordinate with them possible adaptations to the App and the Website accessibility in line with their requirements under the Accessible Information Standard.

Changes to this Policy

This Policy may from time to time be changed by a resolution of the Board of Directors. Its changes shall be made available, and Service Users shall be notified of such changes by means of our Service. Consent of Service Users may be sought in case of more significant changes, or where it might be required by Applicable Legislation.

Changes of the Data Controller, the App or the Website

If we merge with another business entity, the Data may be disclosed to this new business and its authorised personnel, subject to, as a minimum, Applicable Legislation.

Salve Technologies Ltd Information Governance and Security Policy

Information Governance (IG) procedures

The Board of Directors shall appoint from amongst themselves the Caldicott Guardian and the IG Lead, who may be the same person. The Board of Directors shall further appoint a Data Protection Officer (DPO). The DPO shall also serve as the Caldicott Function. The IG Lead and the DPO shall report directly to the board.

The IG Lead shall be responsible for:

a. reporting IG events or incidents e.g. information quality failures, actual and potential breaches of confidentiality, cyber or information security; b. analysing, investigating and upward reporting of events / incidents and any recommendations for remedial action;

c. IG work programme progress reports;

d. reporting annual IG assessment and improvement plans;

e. communicating IG developments and standards to appropriate forum and staff.

To ensure compliance in relation to the changes in legislation, technology and the Service functionalities, the IG Lead or the DPO may at any time propose changes to this Policy to the Board of Directors.

Salve is not a public body and therefore not subject to freedom of information requirements.

The Board of Directors shall pass, and together with the IG Lead / DPO implement, an action plan to ensure that all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual IG Training. Training materials and plans shall be checked for equivalence to materials in the NHS IG Training Tool by auditors or through another documented local governance process. Training shall be regularly reviewed and re-evaluated when necessary. This Policy shall also serve as the Code of Conduct on keeping personal information secure and on respecting the confidentiality of Service Users,

which also includes guidance on the duty to share information for care purposes.

This Policy is public and available to Service Users and our communications strategy includes the ability of Service Users to give their feedback via the Service and the email provided in this Policy, which shall be used as a source for revising and improving the Policy. Our Website shall feature an active communications campaign on ‘fair processing’ tailored to service user needs and co-shaped, to the

extent possible, by Service Users' feedback, that shall set out how personal information is used and shared, plus explain the rights of individuals including the right to object to the sharing or use of confidential information recorded about them.

Information access and sharing requirements and procedures

The Board of Directors shall pass and together with the DPO implement an action plan comprising measures such as criteria, terms and conditions of employment, disciplinary measures in case of data breaches, and action to be taken to protect the Data in case of employment termination.

Audit trails shall be implemented in due course to document access to the Data by individual employees, and such documented trails shall be used as grounds for disciplinary action in case of data breaches.

Regular monitoring and audit of staff confidentiality shall be implemented and performed by the DPO and the IT security personnel and appropriate action is taken where confidentiality processes have been breached or where a near-miss has occurred.

Designated personnel or outside contractors shall be made subject to confidentiality obligations in line with this Policy by means of contractual obligations. In line with the NHS Information Governance Toolkit, appropriate clauses on compliance with IG shall be put into all contracts and/or agreements with third parties before any access to the Data can be granted, or before any transfer or receipt takes place. Such clauses shall adequately address the need for security, policies, staff screening, and training.

To the extent possible by its architecture and subject to the clinic's own privacy policies, the Service enables coordinated and integrated care through appropriate and lawful access by all the relevant clinical staff in charge of the patient.

Any transfers of personal information to countries outside the UK/EU/EEA are documented, reviewed and tested to determine compliance with the Applicable Legislation and the Department of Health (DH) guidelines. This includes a risk assessment with mitigating controls put in place, documenting the transfers (Appendix I), including such transfers in our ICO notification, authorisation of each transfer by the Board of Directors, and obtaining a contractual assurance statement from third parties such as Cloud storage or analytics tools providers who might process data overseas. All such contracts shall be reviewed, wherever possible in advance, before any potential cross-border transfers take place, to ensure that appropriate clauses are included in them or added where it later emerges that they are necessary.

Information Security Assurance Plan

Responsibility for Information Security shall be with the Information Security Officer,

who shall have appropriate formal qualifications, and who shall be appointed by and report directly to the Board of Directors. He or she may be a member of the Board of Directors. The Information Security Officer shall also act as the Senior Information Risk Owner (SIRO) and take responsibility for ownership of information risk across the organisation.

Any additional staff assigned responsibility for Information Security shall be appropriately trained to carry out their role. They shall in their information security role report to the Information Security Officer.

Information Risk Assessment and Management Programme shall be adopted by the Board of Directors and reviewed by the Information Security Officer. Working with

Information Asset Risk Owners and in collaboration with the Board of Directors, SIRO shall identify all business critical systems i.e. Information Assets and processes, including those provided by service contract or agreement such as Cloud storage, and make the relevant Information Asset Owners aware of their responsibilities for analysing their business functions (Information Assets), the effect that disruption may have, and the need to develop Business Continuity Plans for each of their assets.

Contracts or agreements with service providers and business partner organisations shall be reviewed to ensure these include clear reporting requirements, enforceable obligations, expectations and references to procedures for the reporting of and response to incidents.

Data Protection Impact Assessment

Data Protection Impact Assessment shall be performed in relation to any changes in the processing of the Data that are likely to result in a high risk to the rights and freedoms of Service Users or other natural persons.

There shall be a documented procedure and structured approach for ensuring that new or proposed changes to organisational processes or information assets are identified and flagged with an appropriate information governance group or equivalent and that information security, confidentiality and data protection, and information quality requirements are defined at an early stage of the project cycle.

All staff members who may be responsible for introducing changes to processes or information assets shall be effectively informed about the requirement to seek approval from the Board of Directors plus seek DPO advice. All new implementations follow a documented procedure. Where the proposed new process or information asset is likely to involve a new use or significantly change the way in which personal data is handled, an appropriate Data Protection Impact Assessment is always carried out to ensure a robust change control process.

As of 25th May 2018, the rules of Articles 35 and 26 of the GDPR shall apply to Data Protection Impact Assessment in addition to the above.

Data Breaches and Incident Reporting

Information security events, including IG and Cyber Security Serious Incidents Requiring Investigation, must be reported to the Information Security Officer who shall investigate them. In managing information security events, Information Security Officer shall report to the Board of Directors. Data breaches and cyber incidents reaching Level 2 based on HSCIC checklist guidance shall be reported through the IG and Cyber Security SIRI Tool.

All uses and sharing of confidential personal information that do not have a clear legal basis are treated as data breaches and shall be reported to the Board and to the HSCIC via the IG SIRI Incident Reporting Tool.

As of 25th May 2018, we shall also follow Data Breach procedures of Articles 33 and 34 of the GDPR. These shall require us to document and notify the Data breach, without undue delay and, where feasible, not later than 72 hours after having become aware of it, to the ICO or another competent authority, unless the Data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the competent authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Where the Data breach is likely to result in a high risk to the rights and freedoms of natural persons, we shall communicate the Data breach to the Service Users or other affected natural persons without undue delay.