PRIVACY NOTICE

Patient Privacy Notice
Serenity Ultrasound Services Ltd

Document status	*Patient-facing privacy information*
Applies to	*Patients, prospective patients, and people acting on their behalf*
Related services	*Private ultrasound scanning, blood testing, administration, billing, clinical governance and patient communications*
Legal framework	*UK GDPR, Data Protection Act 2018, common law duty of confidentiality, Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, and related guidance*
Related policies	*Records Management Policy and any linked confidentiality, data protection, information security, subject access and retention procedures that Serenity adopts*

Important: This notice explains how Serenity Ultrasound Services Ltd uses personal information. It is designed to meet the transparency requirements of Articles 13 and 14 of the UK GDPR and to provide clear information similar in depth and structure to large healthcare organisations. It is a privacy notice, not a contract, and it does not reduce any rights you have under data protection law.

1. Who we are and the purpose of this notice

Serenity Ultrasound Services Ltd (referred to in this notice as "Serenity", "we", "us" or "our") is a private healthcare provider offering ultrasound scanning, related diagnostic and screening services, blood testing, appointment administration, payment processing, patient communications and associated clinical governance activities. For data protection purposes, Serenity is the data controller for the personal data described in this notice unless we clearly tell you otherwise for a specific service or arrangement.

This notice explains what personal data we collect, why we collect it, the lawful bases and additional conditions we rely on, how we store and protect information, who we may share it with, how long we keep it, and what rights you have. The Information Commissioner's Office states that privacy information should tell people, in a clear and accessible way, who you are, why you use their data, what rights they have, who you share data with and how long you keep it. We have therefore intentionally written this notice in a detailed format so it can sit alongside wider governance documentation and support inspection-readiness as well as patient understanding.

This notice applies when you contact us, book with us, attend for care, complete forms, provide identification or payment information, receive a report or image from us, ask us to liaise with another healthcare professional, make a complaint, request copies of your information, or otherwise interact with Serenity in a way that involves personal information.

2. Data controller details and contact arrangements

Serenity Ultrasound Services Ltd is responsible for deciding how and why your personal information is used. In data protection law this organisation is called the "data controller". Where we use software or service providers such as practice management systems, cloud services, IT providers, laboratories or professional advisers, those organisations may act as our data processors or, in some cases, as separate controllers depending on the activity being carried out and the legal relationship involved.

You may contact Serenity about data protection, confidentiality, subject access requests, corrections, concerns or complaints using the clinic contact details provided to you in your booking information, on our website and in patient communications. If Serenity formally appoints a specific Information Governance Lead or Data Protection contact, this notice should be updated to include that named role and direct contact details. Where this notice refers to contacting us about your data, that means contacting Serenity through the clinic's published contact routes.

3. The types of personal information we may collect

We collect and use different categories of information depending on the service you receive and the reason you contact us. Much of this information is personal data. Some of it, including health information, scan findings and certain pregnancy details, is special category personal data and is subject to stronger protection under UK data protection law.

We may collect identifying and contact information such as your name, former names where relevant, date of birth, age, address, email address, telephone numbers, emergency contact details and, where clinically or administratively necessary, identification information needed to verify your identity or reduce the risk of records being matched to the wrong person.

We may collect administrative and booking information such as appointment details, referral details, GP or referrer information, correspondence, booking notes, payment records, invoices, receipts, communications about attendance or non-attendance, and records of any adjustments requested or required so that we can provide services safely and appropriately.

We may collect clinical and special category information such as symptoms, medical history, medication history, allergies, menstrual history, fertility history, pregnancy history, last menstrual period, previous scan findings,

examination findings, sonographer notes, diagnostic impressions, reports, blood test requests or results, safeguarding information where relevant, and records of clinical discussions, advice, onward referral or escalation.

We may also collect imaging and media information such as ultrasound still images, clips, DICOM studies, thumbnails, reports associated with an examination, and limited patient-access copies shared with you after your appointment. When images or reports are linked to your identity, they are personal data and form part of your health record.

Summary of the main data categories we may process

Category	Examples	Why we use it
Identity and contact data	*Name, date of birth, address, mobile number, email address, emergency contact, GP or referrer details*	*To identify you correctly, communicate with you, administer services and reduce the risk of misidentification*
Clinical and health data	*Symptoms, medical history, scan findings, blood test information, reports, pregnancy details, safeguarding information*	*To provide healthcare safely, create an accurate clinical record, support diagnosis, reporting, escalation and continuity of care*
Imaging and media	*Ultrasound still images, clips, DICOM studies, report-linked images and patient download copies*	*To document examinations, support clinical interpretation, provide reports and offer limited patient access copies where appropriate*
Administrative and financial data	*Bookings, cancellations, attendance history, invoices, receipts, payment references, communications*	*To run the service, manage appointments, take payment and respond to queries or complaints*
Website / communications data	*Web enquiries, email correspondence, SMS reminders and form submissions*	*To respond to enquiries, send service communications and maintain a record of interactions with you*

4. How we collect your information

We usually collect information directly from you when you complete enquiry forms, make a booking, telephone us, email us, attend the clinic, complete consent or health questionnaires, provide identification, provide payment information, or ask us to send results or images. We may also collect information from a person acting on your behalf where that is lawful and appropriate, for example a parent, legal guardian, person with parental responsibility, attorney, translator, advocate or another person you have authorised to help you with your care or booking.

In some cases we may receive information from another healthcare professional, referrer, laboratory, insurer, professional adviser or previous provider. We may also receive information as part of safeguarding activity, complaint handling, incident review, insurance matters, debt recovery where lawful, or regulatory reporting. If we receive personal data from another source rather than directly from you, we will handle it in line with this notice and any additional information provided to you at the time.

5. Our legal bases for using personal information

Under the UK GDPR we must have a lawful basis for processing personal data, and because much of the information we use in healthcare is health data, we must also meet an additional condition for processing special category data. The ICO makes clear that, in healthcare, consent is often not the most appropriate lawful basis for core care records because healthcare providers usually need another lawful basis that more accurately reflects the necessity of using

information to provide care. Clinical consent to an examination or procedure and data protection consent are not the same thing.

For most direct patient care activity, our primary lawful basis under Article 6 is likely to be that processing is necessary for our legitimate interests in operating a safe and effective healthcare service, for performing a contract with you where you have booked and paid for a private service, or for compliance with a legal obligation where this is the most appropriate basis for the activity. For special category data, our primary Article 9 condition is that processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services, carried out by or under the responsibility of a health professional subject to a duty of confidentiality.

We may also rely on other lawful bases and conditions when the context requires it, for example legal obligation for complaints, financial records and regulatory reporting; legitimate interests for basic service communications and protecting the business from fraud or misuse; establishment, exercise or defence of legal claims where a dispute arises; substantial public interest or vital interests in very limited safeguarding or emergency circumstances; and consent where we offer an optional extra that is genuinely voluntary and can be refused without affecting the core healthcare service.

Main lawful bases and additional conditions

Activity	Likely Article 6 basis	Likely Article 9 / additional condition
Delivering private ultrasound and blood testing services	*Contract and / or legitimate interests, depending on the activity*	*Article 9(2)(h) – medical diagnosis / provision of healthcare*
Creating and maintaining clinical records	*Legitimate interests and / or legal obligation*	*Article 9(2)(h) – healthcare provision and management*
Responding to a safeguarding concern or emergency risk	*Legal obligation, vital interests and / or legitimate interests depending on the facts*	*Article 9(2)(h) and, where applicable, other statutory or public interest grounds*
Handling complaints, claims and regulatory enquiries	*Legal obligation and / or legitimate interests*	*Article 9(2)(f) legal claims and / or Article 9(2)(h) where clinically relevant*
Optional marketing communications	*Consent where required by law*	*Usually not special category processing unless content or segmentation involves health data*

6. Pregnancy information and records relating to the unborn child

Where you receive pregnancy-related services, Serenity will create and retain records that may include information about the pregnancy, gestational age, yolk sac, embryo or developing baby, fetal heart activity where visible, placental position where relevant to the examination, measurements, maternal history relevant to the scan, and any findings or recommendations arising from the examination. These records may include images, clips, reports, consent forms and correspondence connected to the pregnancy episode.

The NHS Records Management Code of Practice states that obstetric, maternity, antenatal and postnatal records are retained for 25 years and recognises that such records should be treated as being as much the child's record as the parent's record. Serenity therefore applies an extended retention approach to pregnancy scan records and related imaging because these records may later be relevant to the child as well as to the pregnant patient. Where a record contains information about both the pregnant patient and the unborn child, Serenity will manage that record as a protected health record requiring careful handling, controlled access and a longer retention period.

It is important to understand that a keepsake image or short patient download copy is not the same thing as the legal clinical record. The underlying report, measurements, sonographer notes and retained imaging archive remain the clinical record even if patient-access copies expire or are deleted from a patient-facing sharing method after a limited access window.

7. Children, parental responsibility and third-party involvement

Where services involve a child or young person, Serenity will process information in a manner appropriate to age, understanding, clinical need, parental responsibility and applicable law. We may need to confirm who has parental responsibility or legal authority before sharing information. We may also limit or refuse disclosure where the law allows us to do so, for example if disclosure would risk serious harm, breach another person's rights, or where the young person has capacity and confidentiality applies to their own care.

When another person contacts us on your behalf, we may ask for evidence that they are authorised to do so. This is part of our obligation to protect confidentiality and reduce the risk of disclosing records to the wrong person.

8. Why we use your information in practice

We use personal information to provide safe, effective and well-documented healthcare. This includes triage, booking, confirming identity, understanding the reason for the appointment, obtaining relevant history, performing the examination, generating the report, communicating results, arranging follow-up or onward referral where appropriate, responding to questions, processing payment and maintaining records of care delivered.

We also use information for quality assurance and governance purposes such as audit, peer review, supervision, complaints handling, incident investigation, safeguarding review, insurance reporting, business continuity, system security monitoring, fraud prevention, debt management where lawful, professional regulation and compliance with CQC, ICO, tax, accounting and other legal obligations. CQC Regulation 17 requires providers to securely maintain accurate, complete and detailed records for people using the service, staff employment and the overall management of the regulated activity, so governance record-keeping is an essential and lawful part of operating the clinic.

We will not use your health information for unrelated purposes in a way that is incompatible with the reason it was collected. The ICO's purpose limitation and data minimisation principles require organisations to be clear about why they process personal information and to collect only what is adequate, relevant and necessary for that purpose. Serenity therefore aims to avoid recording irrelevant or excessive information in the patient record.

9. Our main systems, where records are held and how access is controlled

Serenity uses a combination of approved digital systems and controlled local storage. Patient administration and much of the clinical record will be held in Cliniko, including demographic details, bookings, correspondence, consent forms, clinical notes, reports and selected attachments. Cliniko provides user security roles and configurable permissions, and Serenity will use named user accounts, strong passwords, role-based access and the principle of least privilege so that staff only have access to the information they need for their role.

Ultrasound images and related DICOM studies may also be stored in a dedicated imaging workflow using a PACS computer and encrypted hard drives under clinic control. Serenity's intended workflow is that images will be uploaded using approved devices and controlled transfer methods rather than general Wi-Fi-based transfer. This is a risk-reduction measure designed to support secure handling, clearer accountability and controlled ingestion of image files. Where removable media or external hard drives are used, Serenity will use encryption and physical security controls. ICO guidance identifies encryption as an appropriate technical measure, particularly for portable or removable media and for devices that store personal information.

Serenity also uses Microsoft 365 / SharePoint for governance and operational records such as policies, risk registers, staff leave records, incident logs, safeguarding logs, training logs and document control records. Access to these areas will be restricted by permissions, group membership and site or library controls so that sensitive governance records are available only to staff with a legitimate role-based need. Microsoft guidance confirms that SharePoint permissions can be restricted through groups and can be customised at site, library or list level. Serenity will use this functionality to separate staff records, governance records and sensitive logs from broader administrative access.

Some information may exist temporarily in email, secure forms, scanned documents or system exports, but Serenity's intention is always to place the final business or clinical record in the approved record system and avoid unnecessary duplication. Where a duplicate copy exists for operational reasons, it will still be subject to the same confidentiality, retention and disposal controls.

10. Limited patient access to reports and images

Serenity aims to provide patients with convenient digital access to selected reports or images. We may therefore send reports, files or image access links using Cliniko or another approved secure method. This feature is intended to help patients view or download copies for personal use without altering the clinic's underlying legal obligations to retain the official clinical record and imaging archive.

Where patient-access copies are shared digitally, access may be available only for a limited period. Serenity's planned standard access window is up to 30 days from the date the files are made available, unless a shorter or longer period is clearly stated for the specific sharing method. Patients should download and securely save any copies they wish to keep during that period. After the access window ends, the patient-facing link, attachment or portal access may expire or be removed, but the clinic's retained clinical record will continue to be kept in accordance with the applicable retention schedule.

If you need copies after the time-limited sharing window has expired, you may still request access to your records through the normal subject access or records request process. A time-limited download feature is a service convenience, not the only route by which you can lawfully ask for copies of your personal information.

11. Who we may share information with

We will only share your information where there is a lawful and proportionate reason to do so. Depending on the circumstances, this may include sharing with laboratories, referrers, GPs, NHS providers, consultants, insurers, professional indemnity providers, regulators, solicitors, debt recovery providers, software and IT support providers, accountants, secure shredding providers, or public authorities where we are required or permitted by law to do so. We do not sell patient data.

Where an external supplier handles information for us, we expect that organisation to process information only on our instructions, keep it secure, maintain confidentiality and provide contractual safeguards appropriate to the sensitivity of healthcare information. Where another organisation receives information for its own independent purpose, for example a laboratory performing a test requested as part of your care, that organisation may be a separate controller for its own processing and will provide its own privacy information where required.

There may be circumstances where we share information without asking for additional consent because the law allows or requires it. Examples may include safeguarding, prevention or detection of crime, court orders, legal claims, serious incidents or urgent clinical risk. Any such sharing will be limited to what is relevant and necessary in the circumstances.

12. International transfers and cloud suppliers

Some of the digital services used by Serenity may involve storage, access, support or processing outside the UK. Under UK data protection law, transfers of personal information outside the UK are restricted unless appropriate protections are in place. The ICO explains that where an adequacy regulation is not available, organisations may rely on recognised safeguards such as the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, together with a transfer risk assessment where required.

Where Serenity uses cloud-based providers, we will expect those suppliers to offer appropriate contractual and technical measures for international data protection compliance. Cliniko states that it offers a data processing addendum including standard contractual clauses to support GDPR compliance where relevant. Serenity will review and document supplier arrangements as part of its wider data protection and information security framework. This notice should be updated if final supplier arrangements change in a way that materially affects where or how patient data is processed.

13. Security, confidentiality and record integrity

Healthcare information is highly sensitive. Serenity therefore applies a combination of technical, physical and organisational security measures intended to protect confidentiality, integrity and availability. These measures include named user accounts, password controls, limited access based on role, encryption where appropriate, secure devices, system permissions, backups, audit trails where available, restricted physical access to equipment, staff confidentiality obligations, and procedures for incident reporting and breach management.

The ICO's security guidance states that organisations should adopt appropriate technical and organisational measures based on risk, and specifically identifies encryption and storage encryption as useful protections for devices and removable media. CQC also expects records to be accurate, complete, up to date and securely stored and shared. Serenity's approach to records therefore aims not only to keep information confidential, but also to ensure that records remain identifiable, retrievable, attributable to the right person and protected from accidental loss, unauthorised alteration or inappropriate disclosure.

No system can be guaranteed to be completely risk free. However, Serenity will take reasonable and proportionate steps to reduce risk, investigate incidents, learn from errors and notify affected individuals and regulators where required by law.

14. Retention: how long we keep personal information

We do not keep personal information for longer than is necessary, but healthcare records often need to be retained for significant periods because of clinical need, legal requirements, complaint handling, safeguarding, insurance, and the rights of patients and, in pregnancy cases, the future rights of the child. The ICO states that organisations should be able to justify how long they keep information and should have retention schedules or retention policies in place. Serenity's retention periods are therefore set by reference to legal obligations, regulator guidance, business need and the NHS Records Management Code of Practice where relevant to healthcare records.

The tables below summarise Serenity's current intended minimum retention periods. They are minimum periods rather than automatic deletion dates. Records may be held longer where there is an unresolved complaint, claim, investigation, legal hold, safeguarding matter, tax requirement, insurance requirement or other lawful reason to suspend disposal.

Patient record retention summary

Record type	Minimum retention period	Notes

Adult patient health records	*At least 8 years after last treatment or contact*	*Includes core private clinical records unless a longer healthcare-specific period applies*
Pregnancy / maternity / antenatal type records and related scan records involving the unborn child	*25 years*	*Managed on the basis that the record may be relevant to the child as well as the pregnant patient*
Ultrasound images, DICOM studies and associated reports	*Retained in line with the relevant patient record period*	*Patient download copies may expire earlier, but the underlying clinical archive remains retained*
Complaints, incidents or claims linked to patient care	*Normally the longer of the patient record period or the period required for the matter to be concluded*	*May be retained longer where legal proceedings, insurance or safeguarding issues continue*

Operational and communications records connected to patients

Record type	Minimum retention period	Notes
Appointment communications and booking records	*Aligned to the patient record where part of the care record; otherwise normally up to 8 years if needed for administration, complaints or finance*	*Assessed according to whether the information is clinically significant or forms part of the legal record*
Payment records / invoices / receipts	*In line with tax and accounting requirements, usually at least 6 years*	*May also be linked back to the patient account for audit and dispute resolution*
Web or email enquiries that do not progress to treatment	*Only as long as necessary for the enquiry and any related complaint or legal issue*	*Normally retained for a shorter operational period unless converted into a patient record*

15. Your rights under data protection law

Under the UK GDPR you have a number of rights in relation to your personal information. These rights are not absolute and some are limited by healthcare-specific rules, legal exemptions, confidentiality duties and the rights of other people. The ICO states that privacy information should explain which rights apply and, where relevant, should highlight rights such as the right to object separately and clearly.

Your rights may include the right to be informed about how your data is used; the right of access to receive a copy of your data; the right to ask for inaccurate personal data to be rectified; the right to ask for processing to be restricted in certain circumstances; the right to object in certain circumstances where processing is based on legitimate interests; the right to data portability in limited cases where processing is based on consent or contract and carried out by automated means; and rights relating to automated decision-making. In practice, many core healthcare records are not erased simply because a person asks for deletion, because the provider may still need to retain them to comply with legal, professional or regulatory duties.

If you believe information in your record is wrong, Serenity will consider your request carefully. The ICO's accuracy guidance recognises that medical records may include professional opinions recorded at the time and that a disagreement with an opinion does not always mean the record is inaccurate. In appropriate cases, the record may

be corrected, supplemented with an additional statement, or otherwise annotated rather than retrospectively rewritten in a way that damages the integrity of the original clinical record.

16. Subject access requests and copies of records

You can ask us for copies of your personal information by making a subject access request. A request does not have to mention the words "subject access request" to be valid. It can be made in writing, by email and, in many cases, verbally. The ICO states that organisations must normally respond without undue delay and within one month of receiving the request, or within one month of receiving any additional information reasonably required to confirm identity or authority.

To protect confidentiality, Serenity may ask you for proof of identity, enough information to locate the records you want, and, where someone is acting for you, evidence that they have authority to do so. We may provide information electronically where that is appropriate and secure. In complex cases, where the law permits, the response period may be extended or part of the request may be refused if a valid exemption applies. In limited circumstances, we may refuse or charge a reasonable fee for manifestly unfounded or excessive requests, but we would need to justify that decision under ICO guidance.

Where you simply need another copy of a recent report or a previously shared image and the request is straightforward, we may be able to deal with it as a routine records request rather than a formal SAR. However, your underlying legal rights remain the same and the route used will depend on what you are asking for.

17. When we may need to retain, disclose or use information despite a request for deletion or restriction

There are circumstances in which Serenity may lawfully continue to retain or use information even if you ask us to delete it, stop using it, or object to the processing. This may happen where continued retention or use is necessary for compliance with a legal obligation, exercise or defence of legal claims, public interest or safeguarding reasons, regulatory compliance, financial record keeping, complaint investigation, fraud prevention, business continuity or maintenance of the integrity of the healthcare record.

This is particularly important for health records, incident records, safeguarding records, complaints and insurance matters. Requests will always be considered carefully, but the existence of a request does not automatically override a provider's duties to keep accurate records and protect patients, staff and the service.

18. Complaints, concerns and the right to complain to the ICO

If you have a question or concern about how Serenity has handled your information, we encourage you to contact us first so that we can review the matter promptly and try to resolve it. Concerns about confidentiality, inaccurate information, records access, image sharing or data security should be raised using the clinic's normal contact routes.

You also have the right to complain to the Information Commissioner's Office, the UK regulator for data protection matters. The ICO recommends that people raise concerns with the organisation first where possible, but you may contact the ICO at any time if you are dissatisfied with how your information has been handled.

19. Updates to this notice

This notice should be reviewed whenever Serenity changes its systems, services, suppliers, retention schedule, lawful bases, contact details or governance arrangements in a way that materially affects the use of personal information. A review should also take place when relevant law or guidance changes, including ICO guidance, CQC expectations or healthcare records retention guidance.

The most current version of this notice should be made available to patients in a clear and accessible format, including online and within patient information packs where appropriate.

Quick guide to patient rights

Right	What it usually means	Important limits in a healthcare setting
Access	*You can ask for a copy of your personal information*	*We may withhold limited information where a lawful exemption applies, including protection of another person's rights or serious harm considerations*
Rectification	*You can ask us to correct inaccurate personal data*	*Professional opinions recorded accurately at the time may not be "incorrect" simply because you disagree with them*
Erasure	*You can ask for deletion in some circumstances*	*This right is often limited where records must be retained for legal, regulatory, clinical or claims purposes*
Restriction / objection	*You can ask us to limit or reconsider certain processing*	*These rights depend on the lawful basis being used and may not stop necessary healthcare record-keeping*
Portability	*You can ask for data in a reusable format in limited cases*	*Only applies in specific circumstances and does not usually require us to reformat complex clinical archives beyond what the law requires*

Appendix 1 - Plain English summary for patients

- *Serenity keeps records about your appointments, scans, reports, payments and communications so that we can run the clinic safely and provide your care properly.*
- *Your main record will usually be stored in Cliniko, while imaging files such as DICOM studies may also be stored in a secure imaging workflow using a PACS computer and encrypted hard drives.*
- *If we send you images or reports digitally, the link or portal access may only stay live for a limited period, usually up to 30 days. Please download your copies during that time if you want to keep them.*
- *Even if the patient download link expires, the official clinical record is still kept by the clinic for the required retention period.*
- *Adult patient records are generally kept for at least 8 years. Pregnancy-related records are kept much longer, usually 25 years, because the record may also be relevant to the child.*
- *You can ask for a copy of your records, ask us to correct inaccurate information, or raise a concern about confidentiality or security.*

Appendix 2 - Key references used to prepare this notice

This privacy notice has been drafted using UK primary legislation and regulator guidance. Full legal obligations will depend on Serenity Ultrasound Services Ltd's final operating model, suppliers and data flows, and the notice should be reviewed whenever those arrangements change.

1. *Information Commissioner's Office (ICO), Right to be informed and "What privacy information should we provide?" guidance, setting out the minimum information privacy notices should contain.*
2. *Information Commissioner's Office (ICO), A guide to lawful basis; special category data guidance; and guidance stating that in healthcare consent is often not the appropriate lawful basis for core processing.*
3. *Information Commissioner's Office (ICO), Accuracy, storage limitation, data minimisation, security and encryption guidance, including the use of encryption for devices and removable media.*

4. *Information Commissioner's Office (ICO), Subject access request guidance, including timing, identity checks and the handling of manifestly unfounded or excessive requests.*
5. *Care Quality Commission (CQC), Regulation 17: Good governance, and guidance on what good digital records look like, requiring providers to maintain secure, accurate, complete and up-to-date records.*
6. *NHS England / Transformation Directorate, Records Management Code of Practice 2021, including retention schedules and the 25-year retention period for obstetric, maternity, antenatal and postnatal records.*
7. *Cliniko help guidance on UK GDPR support, user security roles, receptionist access controls, secure patient forms and patient file attachments.*
8. *Microsoft Learn and Microsoft Support guidance on SharePoint restricted access control and customised permissions for sites, libraries and lists.*