Data Protection Policy

Policy document defining the Company's Data Protection Policy

CONTENTS

1 INTRODUCTION

1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 Definitions used by the organisation (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data to offer goods and services or monitor the behavior of data subjects who are resident in the EU.

1.3 Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

2 POLICY STATEMENT

Aseptika Limited are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Aseptika collects and processes in accordance with the General Data Protection Regulation (GDPR).

Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.

The GDPR and this policy apply to all of Aseptika's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

The Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to Aseptika's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

This policy applies to all staff of Aseptika and interested parties such as outsourced suppliers. Any breach of the GDPR will be dealt with under Aseptika's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for Aseptika, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Aseptika without having first entered into a data confidentiality agreement which imposes on the third-party obligations no less onerous than those to which is committed, and which gives Aseptika the right to audit compliance with the agreement.

3 RESPONSIBILITIES AND ROLES UNDER THE GENERAL DATA PROTECTION REGULATION

Aseptika is a *data controller and a data processor* under the GDPR.

Senior management and all those in managerial or supervisory roles throughout Aseptika are responsible for developing and encouraging good information handling practices within Aseptika; responsibilities are set out in individual job descriptions.

The Data Protection Officer, a role specified in the GDPR, is a member of the senior management team, is accountable to Managing Director for the management of personal data within Aseptika and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- development and implementation of the GDPR as required by this policy; and
- security and risk management in relation to compliance with the policy.

The Data Protection Officer, who is considered to be suitably qualified and experienced, has been appointed to take responsibility for Aseptika 's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Aseptika complies with the GDPR, as do managers in respect of data processing that takes place within their area of responsibility.

The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for staff seeking clarification on any aspect of data protection compliance.

Compliance with data protection legislation is the responsibility of all staff of Aseptika who process personal data.

Aseptika's IG Policy sets out specific training and awareness requirements in relation to specific roles.

Staff of Aseptika are responsible for ensuring that any personal data about them and supplied by them to Aseptika is accurate and up-to-date.

4 DATA PROTECTION PRINCIPLES

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Aseptika's policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources. The ICO provides guidance on 'Privacy notices, transparency and control' here: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

Aseptika's Privacy Notice Procedure is defined.

The specific information that must be provided to the data subject must, as a minimum, include:

i. the identity and the contact details of the controller and, if any, of the controller's representative;
ii. the contact details of the Data Protection Officer;
iii. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
iv. the period for which the personal data will be stored;
v. the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
vi. the categories of personal data concerned;
vii. the recipients or categories of recipients of the personal data, where applicable;
viii. where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
ix. any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of Aseptika 's GDPR register of processing.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

The Data Protection Officer is responsible for ensuring that Aseptika Ltd does not collect information that is not strictly necessary for the purpose for which it is obtained.

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

The Data Protection Officer will ensure that, on an *annual* basis all data collection methods are reviewed by to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is also the responsibility of the data subject to ensure that data held by Aseptika is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

Staff and clients should be required to notify Aseptika of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Aseptika to ensure that any notification regarding change of circumstances is recorded and acted upon.

The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by Aseptika, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure

The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure). This can be extended to a further two months for complex requests. If Aseptika decides not to comply with the request, the Data Protection

Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will be anonymised in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6 Personal data must be processed in a manner that ensures the appropriate security

The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of Aseptika's controlling or processing operations.

In determining appropriateness, the data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Aseptika itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
    - Role-based access rights including those assigned to temporary staff
    - Encryption of devices that leave the organisations premises such as laptops
    - Security of local and wide area networks

- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Aseptika.

When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout Aseptika;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

Aseptika will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

5 DATA SUBJECTS' RIGHTS

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

Aseptika ensures that data subjects may exercise these rights:

- Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how Aseptika will ensure that its response to the data access request complies with the requirements of the GDPR.
- Data subjects have the right to complain to Aseptika related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

6 CONSENT

Aseptika understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

Aseptika understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

Consent requests must be separate from other terms and conditions and will not be a precondition of signing up to a service unless necessary for that service. Pre-ticked opt-in boxes are invalid – Aseptika will use unticked opt-in boxes or similar active opt-in methods. Consent information will include any third parties who will be relying on consent.

Active consent will be sought through web site, application or through paper consent forms. Consent cannot be inferred from non-response to a communication. Records of consent will be retained as long as the information is held.

For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances, consent to process personal and sensitive data is obtained routinely by Aseptika using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

Where Aseptika provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13).

7 SECURITY OF DATA

All Employees/Staff are responsible for ensuring that any personal data that Aseptika holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Aseptika to receive that information and has entered into a confidentiality agreement

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy). All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy and/or
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media).

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Aseptika. All Employees/Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the record retention procedure.

Personal data may only be deleted or disposed of in line with the retention of records procedure records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

8 DISCLOSURE OF DATA

Aseptika must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police.

The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party; and
- to protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be referred to the SIRO who will seek legal advice where appropriate

9 RETENTION AND DISPOSAL OF DATA

Aseptika shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

Aseptika may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations Aseptika has to retain the data.

Aseptika's data retention and data disposal procedures will apply.

Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

10 DATA TRANSFERS

Aseptika does not transfer data client data outside of the EEA.

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects". The ICO provides guidance on 'Transfers of personal data to third countries or international organisations' here:

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/transfer-of-data/

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

x. An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.* *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

xi. Privacy Shield

If Aseptika wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

10.1 Assessment of adequacy by the data controller

In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

10.1.1 Binding corporate rules

Aseptika may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that Aseptika is seeking to rely upon.

10.1.2 Model contract clauses

Aseptika may adopt approved model contract clauses for the transfer of data outside of the EEA. If Aseptika adopts the *model contract clauses approved by the relevant supervisory authority* there is an automatic recognition of adequacy.

10.1.3 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11 INFORMATION ASSET REGISTER/DATA INVENTORY

Aseptika has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. Aseptika's data inventory and data flow determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of Aseptika throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

Aseptika is aware of any risks associated with the processing of particular types of personal data.

Aseptika assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by Aseptika, and in relation to processing undertaken by other organisations on behalf of Aseptika.

Aseptika shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Aseptika shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

Where, as a result of a DPIA it is clear that Aseptika is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Aseptika may proceed must be escalated for review to the Data Protection Officer.

The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level with GDPR.

APPENDIX A SPECIFIC NHS CONFIDENTIALITY REQUIREMENTS

Common Law Obligations

The Common Law requires that there is a lawful basis for the use or disclosure of personal information that is held in confidence. Unlike the Data Protection Act/GDPR which applies to legal organisations in their entirety, the common law applies to the clinic, team or workgroup caring for an individual, i.e. those not caring for the individual cannot assume they can access confidential information about the individual in a form that identifies them even when they are working in the same organisation.

Normally the basis of access to confidential information will be the consent of the individual concerned and this must be obtained before disclosure or use of the information.

Consent can be implied in some circumstances, but not in others. It is generally accepted that consent can be implied where the purpose is directly concerned with an individual's care or with the quality assurance of that care and the disclosure should not reasonably surprise the person concerned.

Note: Whilst consent can reasonably be implied for direct care in many cases, this is not automatically the case and consent **cannot** be implied when an individual has expressly dissented.

In other circumstances and for other purposes consent cannot be implied and so must be specifically sought or there must be some other lawful basis for disclosing the information.

Sharing Information for Care Purposes

It should be noted that this requirement does not affect the duty to share information for care purposes. This duty was re-asserted by the Caldicott 2 Review Panel in their report 'Information - To share or not to share: The Information Governance Review'. A new **Principle 7,** states that the duty to share information can be as important as the duty to protect patient confidentiality. This means that health and social care professionals should have the confidence to share information in the best interests of their patients/service users within the framework set out by the Caldicott Principles.

Using the Information for Purposes Unconnected to Care Services

The Department of Health response to the Caldicott2 Report placed an expectation on all health and care organisations to:

- Clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes.
- Make clear what rights the individual has open to them, including any ability to actively dissent.

Where an organisation such as Aseptika wishes to disclose confidential personal information for a purpose unrelated to care, **consent cannot be implied**.

In most cases, individuals must be asked for their explicit consent for information to be shared with non-care organisations, for example:

- housing departments;
- education services;
- voluntary services;
- Sure Start teams;
- the police;
- government departments.

Individuals must also be asked for explicit consent for their confidential personal information to be shared for non-care purposes, such as those in Table 1.

Table 1: Non-care purposes
Checking quality of care Testing the safety and effectiveness of new treatments and comparing the cost-effectiveness and quality of treatments in use; Supporting Care Quality Commission audit studies; Comparative performance analysis across clinical networks; and Ensuring the needs of service users within special groups are being met e.g. children at risk, chronically sick, frail and elderly.
Protecting the health of the general public Drug surveillance (pharmacovigilance) and other research-based evidence to support the regulatory functions of the Medicines and Healthcare products Regulatory Agency; Surveillance of disease and exposures to environmental hazards or infections and immediate response to detected threats or events; Vaccine safety reviews; Safety monitoring of devices used in healthcare; Linking with existing National Registries for diseases / conditions; Analysis of outcomes following certain health interventions (i.e. public health interventions as well as treatments); Monitoring the incidence of ill health and identifying associated risk factors; and Identifying groups of patients most at risk of a condition that could benefit from targeted treatment or other intervention.

Managing care services
Capacity and demand planning; Commissioning; Data for Standards and Performance Monitoring; National Service Frameworks; Clinical indicators; Information to support the work of the Care Quality Commission; Evidence to support the work of the National Institute for Health and Clinical Excellence; Measuring and monitoring waiting times, in support of the 18 week target; Data to support Productivity Initiatives; Agenda for Change; and Benchmarking.
Supporting research
Assessing the feasibility of specific clinical trials designed to test the safety and/or effectiveness and/or cost-effectiveness of healthcare interventions; Identification of potential participants in specific clinical trials, to seek their consent; Providing data from routine care for analysis according to epidemiological principles, to identify trends and unusual patterns indicative of more detailed research; and Providing specific datasets for defined approved research projects.

Where explicit consent cannot be obtained Aseptika may be able to rely on the public interest justification or defence. This is where we believe that the reasons for disclosure are so important that they override the obligation of confidentiality (e.g. to prevent someone from being seriously harmed or for safeguarding).

Disclosure may also be required by Court Order or under an Act of Parliament, i.e. there is a statutory or other legal basis for the disclosure. Of particular note in this respect are disclosures permitted under section 251 of the NHS Act 2006, formerly known as section 60 of the Health and Social Care Act 2001. Applications for approval to use Section 251 powers are considered by the Confidentiality Advisory Group (CAG) of the Health Research Authority.

All activities that involve the use or sharing of confidential personal information that do not have a lawful basis must be reported as an IG Serious Incident Requiring Investigation (IG SIRI) using the IG Toolkit Incident Reporting Tool.

In general no-one may consent on behalf of another individual who has the capacity and competence to decide for themselves. However, treating clinicians, parents of young children, legal guardians, or people with powers under mental health law, e.g. the Mental Capacity Act 2005 must make decisions that they believe are in the best interests of the person concerned.

It should also be borne in mind that an individual has the right to change their mind about a disclosure decision at any time before the disclosure is made and can do so afterwards to prevent further disclosures where an activity requires a regular transfer of personal information.

The NHS Care Record Guarantee for England

Individuals' rights regarding the sharing of their personal information are supported by the NHS Care Record Guarantee, which sets out high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

The NHS Constitution for England (revised 2013)

The NHS Constitution sets out a series of patients' rights and NHS pledges. All NHS bodies and private and third sector providers supplying NHS services are required by law to take account of the Constitution in their decisions and actions.

The relevant rights for this requirement are:

- You have the right to be informed about how your information is used.
- You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.

The relevant pledges for this requirement are the NHS commits:

- to anonymise the information collected during the course of your treatment and use it to support research and improve care for others.
- Where identifiable information has to be used, to give you the chance to object wherever possible.
- To inform you of research studies in which you may be eligible to participate.

Where an organisation contracts with a third party to provide care services the contracts must prevent personal information from being used for purposes other than those contracted for and must also ensure that there is explicit consent or some other lawful basis where required. **NB**: Data processor

arrangements and contracts can enable an organisation to share information with a third party working on their behalf, but these do not satisfy the requirements of the common law for there to be a lawful basis before confidential information can be shared with a third party.

Policy: if in doubt, ask the Caldicott Guardian/Data Protection Officer for advice.