1 Introduction

This document sets out Aseptika's approach to managing security, confidentiality, data quality and records.

2 Information Governance Framework

Heading	Notes
Senior Roles	• Senior Information Risk Owner (SIRO) - Managing Director. • Caldicott Guardian – Quality Regulatory & IG Director. • Data Protection Officer - Quality Regulatory & IG Director. • Accountability for record keeping – Quality Regulatory & IG Director.
Key Policies	• Information Security Policy. • Overarching IG policy. • IG staff handbook. • Data Protection Policy. • Network Security Policy. • Record Retention Schedule. All policies and procedures are subject to regular review.
Key Governance Body	Management Meeting.
Governance Framework	Information Governance is discussed at monthly management meetings with a specific agenda set for six monthly management meetings. Attendees of the management meetings: • The Managing Director (SIRO). • Quality Regulatory & IG Director (Caldicott Guardian, DPO, Accountable for record keeping). • Software Developer Manager. • Technical Director. The schedule for covering IG items at the Management Team meeting is set out in Section 4. Information governance requirements are included in staff contracts. Non-disclosure agreements are used where appropriate.
Training & Guidance	An IG staff handbook is in place. The Caldicott Guardian will complete the Role of the Caldicott Guardian Workbook (or e-learning). The SIRO will complete the Introduction to Risk Management for SIROs and IAO's Workbook (or e-learning). All Aseptika staff will undertake e-learning in security and data protection on an annual basis.
Incident Management	See section 13.

3 Responsibilities

3.1 The Senior Information Risk Owner (SIRO)

The SIRO takes overall ownership of Aseptika's information risk policy, implements and leads the risk assessment and management processes and review's the effectiveness of the process.

Key Responsibilities

- Oversees the risk management arrangements and assures that Aseptika remains compliant with NHS Data Protection & Security Toolkit policy, Cyber Essential Plus Certification, Penetration Tests (OWASP Top 10 and OSWAP mobile Top 10) and NHS DTAC standards and methods.
- Takes ownership of the assessment processes for information risk.
- Ensures that Aseptika is kept up-to-date and briefed on all information risk issues affecting the organisation and its business partners.
- Reviews and agrees actions in respect of identified information and clinical data risks.
- Ensures that the approach to information risk is appropriately communicated to all staff.
- Provides a focal point for the escalation, resolution and/or discussion of information risk issues.
- Ensures that identified information threats and vulnerabilities are followed up for risk mitigation and that perceived or actual information incidents are managed in accordance with NHS Data Security & Protection Toolkit, Cyber Essentials Plus, NHS Data Security & Protection Toolkit and NHS DTAC requirements as set out by the Commissioner.
- Monitors compliance with the policy throughout the organisation and develops procedures for effective security.
- Arranges and/or provides information security education and training.
- Develops and monitors a formal procedure for reporting information security incidents and investigations.
- Contributes to the business continuity planning process.
- Advises on the control and monitoring of copying of proprietary software.
- Advises on and monitors the safeguarding of organisational records.
- Ascertains the extent to which information collected, held and/or used in the organisation is properly controlled and safeguarded from loss of confidentiality, integrity or availability from any cause.
- Identifies and tests the controls and, where appropriate, suggests additional controls that will be established to maintain the confidentiality, integrity and availability of information.

3.2 The Caldicott Guardian

Aseptika's Caldicott Guardian is a senior role responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian plays a key role in ensuring that Aseptika staff, along with partner organisations, satisfy the highest practicable standards for handling patient identifiable information. Acting as the 'conscience' of Aseptika, the Caldicott Guardian actively supports work to enable information sharing, where it is appropriate, to share and advises on options for lawful and ethical processing of information.

The Caldicott Guardian represents and champions confidentiality requirements and issues at management meetings.

In this role the Caldicott Guardian will be responsible for ensuring that internal audits of data confidentiality are undertaken.

Key Responsibilities

- Ensures that patient consent forms are provided to patients.
- Ensures that patient's requests for access to their own information are processed in a timely manner.
- Ensures that any patient (clinical) information released to external organisations are subject to suitable pseudonymisation prior to being released or as applicable.
- Reviews existing flows of patient information.
- Reviews database construction and management where any patient information is stored.
- Reviews procedures for handling patient-identifiable information generally, including information collected by Aseptika and used in its dealings with other organisations, e.g. during clinical trials or providing services to the NHS or Local Government Authorities (LGA).
- Defines escalation and handling procedures for any information breaches, including the need to notify other organisations.
- Develops an improvement plan to address any identified deficiencies.

3.3 Data Protection Officer (DPO)

The DPO will drive compliance with the UK General Data Protection Regulation (UK GDPR), where appropriate EU GDPR and ensures ongoing compliance of all core activities for Aseptika.

Key responsibilities

- The Data Protection Officer maintains expert knowledge of data protection law and practices, as well as other professional qualities to ensure that Aseptika complies with the requirements of the UK GDPR, where appropriate EU GDPR and relevant data protection law(s) and regulations.
- Reports directly to Managing Director, the DPO informs and advises on the protection of personal data in relation to the UK GDPR and EU GDPR and relevant law(s) and regulations.
- The DPO ensures that documentation to demonstrate compliance with the GDPR, such as policies and procedures, are kept up-to-date. For example, the register of processing required under Article 30.
- Furthermore, the DPO plans and schedules data processing audits regularly, monitoring core activities to ensure they comply with the UK GDPR, where appropriate EU GDPR.
- The DPO is the main contact point for employees and liaises with all members of staff on matters of data protection and privacy.

Key tasks of the Data Protection Officer (Article 39, (1) and Recital 97)

a) Informs and advises all members of staff on their obligation to adhere to the UK GDPR, where appropriate EU GDPR, and relevant law(s) when dealing with personal data.
b) Monitors compliance with the UK GDPR, where appropriate EU GDPR, and relevant law(s).
c) Advises and informs on the privacy impact assessment (PIA) and data protection impact assessment (DPIA), including monitoring performance of PIA and DPIAs against the requirements of the UK GDPR Article 35, where appropriate EU GDPR.
d) Liaises and cooperates with the supervisory authority.

e) Is the point of contact for the supervisory authority on issues relating to processing of personal data and consults with the supervisory authority, where necessary, on any other personal data matter.

f) Contributes to the development and maintenance of all Aseptika's data protection policies, procedures and processes in relation to the protection of personal data.

g) Advises management on the allocation of responsibilities internally to support ongoing compliance with the UK GDPR and UK law(s), where appropriate EU GDPR.

h) Ensures training and awareness is available and delivered to all members of staff involved in processing operations relating to personal data.

i) Regularly monitors compliance with the UK GDPR, where appropriate EU GDPR, and relevant data protection law(s) by conducting audits of processes relating to personal data and report to the Managing Director.

j) Is the point of contact for data subjects about the processing of their personal data.

k) Monitors compliance with the Data Protection Policy and to develop/advise on procedures for effective security.

l) Advises senior management on the allocation of information security responsibilities.

m) Develops/advises on formal procedures for reporting incidents (UK GDPR and information security-related) and investigations under Articles 33 and 34 of the UK GDPR, where appropriate EU GDPR.

n) Contributes to the business continuity and disaster recovery planning process.

o) Advises on and monitors the safeguarding of organisational record management and Retention of Records Procedure.

p) Ensures that records of the processing are kept by Aseptika as detailed in Article 30 mentioned above.

q) Advises the data controller of its obligation to issue privacy notices to data subjects at the point of collection of their personal data under Articles 13 to 15.

4 Management Meetings

4.1 Monthly IG Improvement meetings

In monthly meetings we review:

- Changes in the environment, which may affect IG (e.g. new contracts, resourcing).
- Role-based access audits.
- New risks / update on risk issues.
- Incidents/issues.
- Data quality issues.
- Audits undertaken.
- Privacy Impact Assessments.
- Data Protection Impact Assessments.
- Caldicott Guardian issues.
- Annual training completion.
- AoB.

Note. Any agenda item for which there is nothing to discuss will be noted accordingly.

4.2 Six monthly meetings

Six monthly meeting (1)	Six monthly meeting (2)
Review • IG Management Framework. • IG Policy. • Business Continuity Plan. • Review any changes required to the Staff IG Handbook. • Review user access.	• Review asset register. • Review of acceptable risks. • Review supplier list. • Data flow mapping. • Review adequacy of training arrangements.

5 Contractual Requirements for Staff and Third-party Suppliers

Aseptika ensures that it fulfils its legal and other responsibilities regarding confidential information and confirms that all staff members (including temps, locums, students and volunteers) and third-party contractors with access to Aseptika's information or systems are fully informed of their own obligations to comply with information governance requirements for security and privacy.

Aseptika includes a specific and explicit clause in the contract of employment, volunteer agreement or contract for services (e.g. IT services) stating an obligation to keep personal information confidential. Where Aseptika signs service agreements (e.g. hosting arrangements), it ensures that the security and privacy arrangements required are appropriately addressed in the agreement.

The contract also provides a formal record that Aseptika has taken steps to ensure that staff recognise their own responsibility for protecting health and care information.

Where appropriate an individual or third-party are required to sign a non-disclosure agreement.

Breach of confidence, inappropriate use of patient/service user records or abuse of computer systems may lead to disciplinary measures.

Aseptika's policy allows the undertaking of audits of personnel records, contractor and other third-party contracts to determine how many have written contracts and of those, which contain clauses that identify responsibilities for information governance, linked to disciplinary procedures (where appropriate).

Where any gaps exist, a process is implemented to ensure that appropriately worded clauses are issued to, signed and incorporated within the contracts of existing staff, contractor and third-parties and all new members of staff and new contracted third-parties sign a contract containing an IG clause.

Contracts with third-party data recipients always include a clause requiring incidents to be reported to the data provider.

A copy of Aseptika's third-party Non-Disclosure Agreement is available. Key relevant items include:

Key components of third-party non-disclosure agreements
Specific reference to Data Protection and security issues, such as: • Notification of the fact of processing data to the IG Lead. • Obligations to comply with limits set by Aseptika. • The security and data protection standards that apply to both parties. • Whether the contractor can act independently or only on instruction from Aseptika.
Additionally: • Penalties for breach of the non-disclosure agreement. • A provision to indemnify the organisation against breaches by the third-party. • Responsibilities for costs, e.g. for security audit, subject access for handling information requests. • Incident-reporting requirements, contracts with third-party data recipients must include a clause requiring incidents to be reported to the data provider.

Our primary security process is not to allow third-parties access to any patient-related data unless necessary.

6 Sharing Confidential Information

Aseptika's data protection policy provides conditions that are met when processing personal information in-house. In addition, where personal information is held in confidence (e.g. details of care and treatment), the Common Law Duty of Confidentiality requires the consent of the individual concerned or some other legal basis before it is used and shared by Aseptika staff. Staff must be made aware of the right of an individual to restrict how confidential personal information is disclosed and the processes that they need to follow to ensure this right is respected.

Aseptika gains consent from system users for sharing of data (with a healthcare professional) through its applications, see the PIA and DPIA's for Aseptika's App products. Aseptika does not routinely share information for care purposes, except for a contracted service or consented clinical trial or equivalent. The consent is the responsibility of the systems users. If, during training the system users use of the equipment, a staff member has serious concerns of a user's health, the staff member must seek consent from the user to contact a healthcare professional. If the individual is unable to consent through illness or incapacity, advice must be sought from the Caldicott Guardian within Aseptika. In all circumstances the matter and actions taken will be recorded as an incident.

6.1 Use and Disclosure of Personal Information

Where a care organisation is using and disclosing personal information for purposes relating to the care of an individual, the Data Protection Act 2018 will not prevent that use or disclosure. Aseptika gains consent from system users for sharing of data (with a healthcare professional) through its applications, see the DPIA's for Aseptika's App products. However, other uses or disclosures are likely to require the explicit consent of the individual concerned and this consent is sought by those organisations separately from the use of Activ8rlives Apps.

Any queries on sharing personal information must be raised with the Data Protection Officer DPO/Caldicott Guardian or another member of the senior management team in the absence of the DPO.

See section 10 for transfer of personal and sensitive information.

6.2 Requests from system users for inform on their records or access to their records

Requests are directed to the Data Protection Officer (DPO).

7 Access Control (See also the Network Security Policy)

Aseptika has access control in place, which includes Aseptika's staff access to confidential patient/service user/customer information for specific purposes, which are fully audited and reported at the time of access and then discussed during Aseptika's monthly IG Improvement Meetings.

The principle of least access is adopted for the design and operation of systems to control access to patient and their data.

Systems are designed and configured to support user access controls and auditing.

Special attention is given to managing access rights, which allow support staff to override system controls. See ASL IG P-014 Role Access Requirements.

Aseptika's computer systems have multi-factor authentication Login procedures that includes at least a unique user ID and password. The following features are implemented:

- System/application identifiers will not be displayed until the Login procedure has been successfully completed.
- The Login does not indicate which part of the Login information is incorrect, e.g. if a user makes an error. This prevents unauthorised users identifying patterns when attempting to gain access to systems.
- Aseptika limits the number of unsuccessful consecutive Login attempts to six. A pop-up window then advises the user to contact the Aseptika helpdesk to have the password reset. The system is also set to record unsuccessful Logins (useful to identify frequency of errors and to be alerted to the possibility of a hacking attempt).
- Limits the maximum time allowed for Login.
- The system records the date and time of successful Logins. Audit Logs can and will be used during investigations. The Audit Log is, therefore, a valuable source of evidence and should be linked to a workstation identity (see ASL IG F-007 MAC address registry).
- The password being entered is not displayed in clear text.
- Passwords are not transmitted in clear text over a network. Passwords are encrypted through, for example, an RSA or hashing algorithm for transmission over networks.
- Systems enforce password changes after a specified period of time.

7.1 Identifying and Authenticating Users

In order to facilitate and operate effective access control and audit functions it is possible to uniquely identify all users of an information asset. This function is achieved by unique username and password combination or, in systems containing sensitive information, secondary smart token technology and biometrics.

7.2 Password Management System

Password management systems are used to establish rules concerning the use of passwords in the Aseptika system. The following criteria are implemented:

- In all but exceptional circumstances, all users are identified as individuals (including system administrators) when they Login.
- Users have to change their initial password (issued by the system administrator) following their first Login.
- Web browsers are configured to prevent the recording of website passwords when logging into a web-based applications. Recording of website passwords renders the password ineffective as a security measure. Passwords are, therefore, most effective if manually entered by the user at each Login.
- The system prevents password re-use.
- Quarterly password changes are enforced, re-use of passwords is prohibited and passwords must meet the following requirements:

  - ✓ A minimum of eight characters in length.
  - ✓ Differs from the associated username.
  - ✓ Contains no more than two identical characters in a row.
  - ✓ Is not a dictionary word.
  - ✓ Includes both numeric and alphabetic characters.

- Password data is stored separately from application data.
- Password is hashed and salted.

7.3 Use of System Utilities

System utilities is restricted by access control and disabled if not required.

7.4 Session Time Out

Session timeouts are implemented where possible.

Aseptika staff members can access the internet for limited private purposes, e.g. email or web browsing. See the staff handbook (ASL IG P-020 Staff Handbook). The use of web email and the browsing of ‘untrusted’ web sites may potentially introduce risks, for example, the download of malicious code (spyware, viruses, worms, etc.) or the viewing/sharing of inappropriate or illegal material. Therefore, Aseptika has formal (see ASL IG P-020 Staff Handbook) policies, which detail staff obligations and undertakings for acceptable use.

Users of Activ8rlies.com and applications must acknowledge (digitally or in writing) 'acceptable terms of use' documentation or similar as part of the registration process. This explains the user rights in unambiguous terms and the user is required to sign a form to acknowledge they have read, understood and agree to these terms.

User training documentation, guidance and the provision of user training sessions is an integral part of the user registration process.

7.5 Review of User Access Rights

Aseptika user access rights are subject to regular review.

8 Storage of Personal Information

Aseptika's policy is to hold all client health data in the UK. Software as a service application, which may hold employee data, is subject to risk assessment and mitigation (for example through contract) as required.

9 Ensuring Privacy and Security

Aseptika ensures that when new processes, services, systems and other information assets are introduced that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements.

A range of activities will be undertaken to fulfil this objective including:

- Aseptika undertake formal privacy and data protection impact assessments to ensure that data protection and security issues are identified and mitigated at the project/initiative outset, see ASL IG P-039 Privacy Impact Assessment PIA and ASL IG F-022 Data Protection Impact Assessment DPIA.
- Aseptika undertake mapping and flows of data and ensure that security is in place for these data flows, see ASL IG F-011 Data Workflows.
- Aseptika deploys encryption in response to assessed risk, contractual, legal or regulatory requirement, see ASL IG P-011 Encryption Policy and Procedures.
- Aseptika always develop IT systems to ensure data integrity and privacy by design, see ASL IG P-018 Privacy By Design.
- Aseptika undertake development and testing outside of the production systems, see ASL IG P-006 Software Test and Release Policy.
- Aseptika establish a fall-back arrangement for system and application changes, see ASL IG P-012 Business Continuity Plan.
- Aseptika implement formal approval of changes to products and system, through our change control process in our Quality Management System.

10 Transfers of Personal and Sensitive Information

Aseptika ensures that all transfers of personal and sensitive information (correspondence, faxes, email, telephone messages, transfer of patient records and other communications containing personal or sensitive information) are conducted in a secure and confidential manner. This ensures that information is not disclosed inappropriately, either by accident or design, whilst it is being transferred or communicated to, within or outside of the organisation.

10.1 Defining Personal and Sensitive Information

Personal Information. This relates to information about a person, that would enable that person's identity to be established by one means or another. This might be fairly explicit, such as an unusual surname or isolated postcode or items of different information, which if taken together could allow the person to be identified. All information that relates to an attribute of an individual is considered as potentially capable of identifying them to a greater or lesser extent.

Sensitive Information. This can be broadly defined as that, which if lost or compromised, will affect individuals, organisations or the wider community. This is wider than but includes information defined as sensitive under the Data Protection Act 1998, e.g. an individual's bank account details are likely to be deemed 'sensitive', as are financial and security information about an organisation.

10.2 Movement of Personal and Sensitive Information

Information is commonly moved around and between organisations, whether in paper health records, in electronic form or on other media. Where this information is personal or sensitive information, Aseptika transfers these with appropriate regard to its security and confidentiality. We also ensure that the media are protected from unauthorised access and environmental damage at all stages of the move. External exchanges are carried out based on agreements between the exchanging organisations.

Aseptika's procedures and standards to protect information and media (paper, electronic storage media, etc.) in transit are well established (see ASL IG P-017 Data Protection Policy). The business and security implications associated with transferring information electronically, e.g. by email are always considered.

Aseptika has procedures in place to ensure all personal and sensitive information relating to patients/service users is received to a secure and protected point (ASL IG P-017 Data Protection Policy). These secure points, also referred to as 'safe havens', are in place wherever the information is received, including transcribing of phone messages, fax in-trays, electronic mailboxes, pigeon-holes and in-trays for paper information etc.

10.2.1 Appropriate Transfer Methods

Aseptika's guidelines on appropriate transfer and protection measures are provided below under the following headings:

Encryption. Encrypted electronic media transported between sites or organisations are properly packaged and clearly labelled to ensure they are handled correctly and not corrupted by magnetic fields (ASL IG P-011 Encryption Policy and Procedures).

Email. Email is not a secure system. All Aseptika staff using email are made aware of this during their induction training and during any training provided for use of the email system. Therefore, patient identifiable and other sensitive information is not sent between organisations unless it has been encrypted to standards approved by the NHS.

Email communication directly with clients/patients/service users is only undertaken with the consent of the client/patients/service users, who will be informed that the security of email cannot be guaranteed.

Emails containing patient identifiable information are stored appropriately upon receipt by Aseptika, e.g. incorporated within the individual's record and deleted safely from the email system when no longer needed.

Email attachments are one of the most common methods for transmitting viruses. All Aseptika staff are informed of the dangers posed by opening attachments, especially those they were not expecting. Up-to-date anti-malware software that includes anti-virus capability, are installed and configured throughout Aseptika's IT network and computing equipment for on-access scanning. Fortnightly checks of all staff laptops and systems ensure that all software and anti-virus capacity is current.

10.3 Procedures and Guidance for Staff

Before transferring information, Aseptika staff always obtain answers to the following questions:

- Is there a valid need to use/disclose confidential information?
- Is it necessary to use confidential information?
- Has the minimum possible confidential information been used?
- Do the proposed recipients need to know all the confidential information?
- Have all staff members been informed of their responsibilities for protecting confidential information?
- Is the use of confidential information lawful?
- Does the stated purpose for transferring the information make it more important that the information is shared rather than withheld?

Staff also consider:

- How much information can be given, e.g. on the phone?
- Where and how incoming messages are recorded, e.g. a message book?
- When a particular type of mail route may be used, e.g. email.
- When a courier should be used.
- Discussion of patients in public.

All areas from which correspondence, email, telephone messages, transfer of patient records and other communications containing personal information may be sent are identified and data flows are risk assessed for security.

11 Network Operations for Secure Information Communication Technology (ICT) Networks

Aseptika maintains a network security policy to ensure that access to network and network services are secure, see also the network policy (ASL IG P- 009 Network Security Policy).

11.1 Policy and procedures ensure that mobile computing and teleworking are secure

Specific requirements for home working are set out in the Aseptika's staff handbook and reinforced during induction for new staff and during the annual IG training for all staff. Remote connections to Aseptika systems, data backup arrangements and system update requirements are set out in the Network Security Policy.

Staff may be required to work in remote locations and must consider the following before accessing the Aseptika systems:

Theft, Loss or Damage of Equipment. Users must not leave equipment in a place where it is vulnerable to theft, e.g. unattended in public areas or on the back seat of a car.

Unauthorised Access to Data. Remote workers must lock their screen or close down their system when away from their device. Staff must consider who can view the details on screens, in public locations and use a privacy screen for their device if required.

Encryption. Any digital information that is either personally identifiable or otherwise sensitive, must be encrypted. This instruction applies to both the storage of and transfer of any such digitally held information by Aseptika staff.

Overheard information. Aseptika's business is not to be discussed in public areas (e.g. trains, cafés) or on remote/client sites where conversations may be overheard by individuals with whom the conversation is not intended.

12 Information Asset Register

Aseptika maintains registers of all information and information assets, including information, software, physical assets and services including web-based services. Asset registers identify the asset owners (see ASL IG F-012 Information Assets Register).

13 Physical Security

Aseptika ensures that the organisation's assets, premises, equipment, records and other assets including staff are protected by physical security measures. The network security policy (see ASL IG P-009 Network Security Policy) identifies the measures Aseptika staff must take to protect network equipment/rooms.

13.1 Securing the Premises

Aseptika office areas and areas containing IT equipment have physical access restrictions in place that are appropriate to information/equipment within the area. Staff are responsible for ensuring that physical security measures are maintained, e.g. doors are closed, locked and alarmed as required.

13.2 Window Security

Windows are locked and a risk assessment is undertaken to determine if blinds or shutter systems are required. Aseptika staff are responsible for ensuring that windows are locked (where required) blinds are drawn and suite entrance door is locked and office security enabled at the end of the day.

13.3 Alarms

The Aseptika office premises are protected by CCTV, burglar and fire alarms, which are regularly tested and monitored by a Keyman service appointed by the Landlord.

13.4 Keys and Staff Access

Physical keys and security access tokens are issued to staff and visitors to the Aseptika offices on a need-to-have basis and logs of issues, returns and lost access keys and security access are maintained.

13.5 Clear Desk and Clear Screen Policy

Staff are encouraged to clear desks of any sensitive and confidential information when it is no longer required for the task in hand and to ensure that such information is locked securely away overnight. Staff must disable screen savers and screen lock their device when the device is left unattended.

13.6 Disposal of paper media

A shredder is provided, which must be used for disposal of Aseptika, client or business partner confidential information.

13.7 Assessment of Physical Security

A risk assessment of physical security is undertaken on an annual basis as a minimum. The physical security is risk assessed constantly to ensure the physical security of Aseptika's environment.

13.8 Steps to Take Following Unauthorised Access

Any breach of physical security is recorded as a non-conformity and a member of the management team is informed immediately.

14 Business Continuity Plans

Aseptika maintains a business continuity plan to ensure the availability of critical business processes (see ASL IG P-012 Business Continuity Plan).

15 Incident Management and Reporting Procedures

Information incidents include a loss/breach of staff/patient/service user personal data, a breach of confidentiality or other effect on the confidentiality, information security or quality of staff/patient/service user information.

All incidents and near-misses are reported, recorded and appropriately managed so that where incidents do occur, the damage from them is minimised and lessons are learnt from them. Incidents are reported via the incident reporting procedure (see ASL IG P-004 Information Incident Reporting Procedure).

16 Risk Management

Aseptika's risk is managed through organisational change activity, for example undertaking privacy and data protection impact assessments and a formal risk management process, which assess the risk to information assets using a defined assessment criterion. Risks are recorded on a risk register (see ASL QM F-710-004 Risk Management Record). Any new risks are reviewed at monthly IG Improvement meetings and all existing risks are reviewed on an annual basis or as required.

17 Record Quality

Aseptika systems capture information directly from application users, who are responsible for their own data accuracy. The validation and range checks on data input are built into Aseptika's applications. Software development and testing identify integrity issues, which are then addressed before systems are released to the production environment.

Integrity issues identified by users are addressed under the incident reporting procedure.

18 References

ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems
BS EN ISO/IEC 27701:2021	Information Security Techniques - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
ISO 27033-6 IEC/EN 2016	Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems
BS EN ISO/IEC 27701:2021	Information Security Techniques - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
WCAG 2.1	Web Content Accessibility Guidelines 5 June 2018
NHSx DTAC	Digital Technology Assessment Criteria
NHS	The Information Security Management: NHS Code of Practice April 2007
NHS DSPT	NHS Data Security & Protection Toolkit
Cyber Essential	Cyber Essentials & Cyber Essentials Plus
ICO.org	Personal data breaches: Information Commissioners Office
ICO.org	The Information Commissioner’s Office (ICO) Guide to Data Protection
MDCG 2019-16 Rev.1	Guidance on Cybersecurity for medical devices

19 Document History

Version	Date	Authors Initials	Reviewers Initials	Changes from Previous Version	Authorised by & date
2.0	12.02.2018	Gareth Lawrence		Major new draft	
2.1	12.02.2018	KAA		Document Control Page added	
2.2	14.02.2018	KAA		Formatting	
2.3	15.02.2018	KAA		Policy number added	
2.4	16.02.2018	JMA		Updating	
2.5	28.2.2018	KAA		Updated as Public document	
2.6	02.05.2018	ETRA	KA	Updating the password management and to a new template	
3.0	11/12/2018	ETRA	KAA, JAA, CB	Annual review and part of CC2018-0187	
4.0	02.12.2019	JA	Kevin Auton /MP	MDR Transition update, part of CC2019-057	
5.0	29.10.2020	JA	MP	Update as per CC2020-059	KAA
6.0	22.11.2021	JA	GE	Annual review, CC2021-075	Kevin A Auton

					23.12.2021
7.0	07.03.2022	JA	GE	Update language CC2022-018	Kevin Auton 18.03.2022
8.0	01.07.2022	JA	GE	Update CC2022-041	KAA 04.07.2022
9.0	27.10.2022	JA	GE	Migrate to AWS CC2022-063	KAA authorise JA 02.11.2022