BrisDoc Patient care by people who care

NHS

Information Governance Framework

Version:	Owner:	Created:
2.4	Debs Lowndes (Programme and Service Director)	March 2010
Published:	**Approving Director:**	**Next Review**
8th April 2024	Nigel Gazzard (Managing Director)	March 2026

Contents

Information Governance Framework

1. Purpose & Principles

The Information Governance Management System (IGMS) is a set of policies brought together to set minimum standards and policy direction in relation to security, confidentiality, integrity and availability of information BrisDoc is responsible for:

- Monitoring, maintaining and improving compliance with appropriate legal and regulatory requirements.
- Developing, maintaining and monitoring the integrity of information to ensure that it is of sufficient quality for use within the purposes it was collected.
- Developing appropriate resilience and recovery arrangements for systems, based on assessed risks to information and its perceived value, to ensure that availability of information is not compromised.
- Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles
- Ensuring the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.
- Ensuring technology is secure and up-to-date.
- Encouraging clinicians and other members of care teams to share information to enable joined-up care, better diagnosis and treatment where possible
- Ensuring there are no surprises to the citizen about how their health and care data is being used and that they are given a choice about this.

Staff are responsible for:

- Maintaining physical security of the building whilst on duty.
- Maintaining security of identifiable information at all times.
- Ensuring they understand Caldicott and Data Protection principles.
- Completing training by the required dates
- Being aware of and behaving in accordance with policy.
- Reporting incidents and near misses to their line managers or service Caldicott Leads via BrisDocs incident Portal.

2. Scope

The IGMS covers all aspects of information, including (but not limited to:)

- Patient/Client/Service User/Citizen information
- Staff related information
- Organisational information

The IGMS covers all aspects of handling information, including (but not limited to:)

- Information held in structured record systems (paper & electronic)
- Transmission of information (fax, email, post & telephone)

- Retention and disposal of information
- Staff conduct relating to the use of information in any form

The IGMS covers all information held, created or accessed by employed staff, or any other party, performing activities in conjunction with the business of the organisation.

3. BrisDoc's Information Governance Management System (IGMS)

The IGMS has been set out as a compilation of component policies that comprises of this document and the following documents:

3.1 Corporate Governance

Where available: Company intranet, shared drives and USB at bases.

Corporate Governance is integral to how BrisDoc operates, ensuring we deliver our services to the highest standards, in an open, honest and proper way, adopting best practice and adhering to legal and regulatory requirements.

The document describes the corporate governance processes that help BrisDoc to assure the quality of our business and how we do things.

3.2 Staff Information Governance Awareness and Training

Where available: Company intranet, shared drives and USB at bases..

This document focuses on how staff are made aware of their responsibilities in connection to Information Governance legislation via three main stages: before employment; during Induction; and ongoing training / awareness.

This policy also explores how BrisDoc measures compliance of its staff.

3.3 Third Party Confidentiality Agreement

Where available: Company Head Office shared drives.

This agreement is to be signed by any Contractor supplying services to BrisDoc who may have access to confidential Information held by BrisDoc about its own business and about patients, employees and other Contractors. These will include third parties who are located on-site on any of the BrisDoc premises or who may have access to BrisDoc's computer systems and data via remote access for any period of time as defined within their contract.

They could include the following:

- Hardware and software maintenance companies
- Cleaning, catering, security guards and other outsourced support services

3.4 Information Security

Where available: Company intranet, shared drives and USB at bases.

The purpose of this policy is to provide clear direction, support and commitment to maintaining the confidentiality, integrity and availability of information obtained, held, used and shared by BrisDoc.

3.5 Mobile Computing

Where available: Company intranet, shared drives and USB at bases.

This document covers the use of all mobile computing devices. This includes but is not restricted to laptops, notebooks, memory sticks, external hard drives and advanced mobile phones. The policy applies to all staff.

3.6 Smartcard Policy

Where available: Company intranet, shared drives and USB at bases.

The purpose of the Smartcard Policy is to, inform individuals of their responsibilities, monitor compliance and inform individuals of the process of dealing with misuse (Disciplinary Action). It sets out the required actions to ensure users comply with Terms and Conditions of Smart Card use.

3.7 Network Security

Where available: Company intranet, shared drives and USB at bases.

The purpose of this document is describe the Network Security Policy that applies within BrisDocs IUC Service. The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

3.8 Incident Reporting

Where available: Company intranet, shared drives and USB at bases.

This information governance supporting policy for part of BrisDocs risk management framework and describes the processes for reporting and managing incidents.

3.9 Data Protection by Design

Where available: Company intranet, shared drives and hard copy at bases.

This policy describes the mechanisms for managing and impacting new or changes to systems, via a change management control system that is based on an accurate and up to date Information Asset Register which lists all of the information systems, current data depositories and data bases used in the delivery of the service. This will ensure that any security, confidentiality, data protection and data quality issues have been considered for any new or reconfigured asset, system or procedure.

3.10 Business Continuity/Disaster Recovery

Where available: Company intranet, shared drives and USB at bases.

This policy describes the roles and responsibilities and actions plans that need to be carried out in the event of one of a number of scenarios occurring at one of the PCCs.

3.11 Data Flow Mapping & Information Asset Register

Where available: Company shared drives.

The tool documents all data flows of person identifiable and business sensitive information and the supporting information assets held to enable the business of BrisDoc. The data flows, shows us how information moves through the organisation and the information asset register how it is stored. All flows and information assets are documented and reviewed in terms of access controls, business continuity, and risk assessment. The tool is maintained by the IAO in conjunction with the IAAs.

3.12 Access to Health Records

Where available: Company intranet, shared drives and USB at bases.

The purpose of this document is to detail the process and responsibilities for dealing with Patient requests to personal information within BrisDocs IUC Service.

3.13Monitoring Access To Patient Information

Where available: Company intranet, shared drives and USB at bases.

The purpose of this document the detail the confidentiality audit procedures that apply within BrisDocs Services.

3.14 Records Management

Where available: Company intranet, shared drives and USB at bases.

The purpose of this policy is to actively encourage and support BrisDoc and define the process for excellent record keeping, both in its clinical and non-clinical environments.

3.15 Data Protection, Confidentiality& Disclosure Policy

Where available: Company intranet, shared drives and USB at bases.

This policy provides guidance to ensure that all patient information is processed fairly, lawfully and as transparently as possible so that the public:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information;
- gain trust in the way BrisDoc handles information and;
- understand their rights to access information held about them.

3.16 Email and Faxing Operational Guidance

Where available: Company intranet, shared drives and USB at bases.

This document sets operational guidance for email and faxing. Each is dealt with separately but overall responsibilities and legal requirements apply to both. All information is in regards to the sending of patient/person identifiable, corporate and sensitive data. Information Governance Leads for each service / department are identified above and should be contacted if you are in doubt.

3.17 Data Sharing with 3rd Parties Pseudonymisation and Anonymisation Policy

Where available: Company intranet, shared drives and USB at bases.

The purpose of this policy is to provide guidance when preparing data extracts to share with third parties, to ensure that the secondary use of patient data is done so in a legal, safe and secure manner e.g. CCGs and universities/health bodies for research purposes.

3.18 Social Media Policy

Where available: Company intranet, shared drives and USB at bases.

This document sets operational guidance for use of social media in BrisDoc.

3.19 Home Working Policy

Where available: Company intranet, shared drives and USB at bases.

The policy sets out the framework for homeworking within BrisDoc.

3.20 Data Breach Notification Procedure

Where available: Company intranet, shared drives and USB at bases.

The document sets out the data breach notification procedure.

4. Other information available to staff that is included as part of the induction process

- The **Caldicott Principles** Leaflet is based on NHS Digital content and is given to staff at induction.
- The **DPA 2018 Overview Leaflet** is from the Department of Digital, Culture Media and Sport content and is given to staff at induction.
- The **BrisDoc Code of Expectations and Behaviour,** which is available on the BrisDoc intranet. This document outlines BrisDoc's expectations of staff when working for the organisation and is given to staff at induction.

5. Other Related policy & code(s) of practice

- Workforce Policies – In setting out standards relating to Information Governance a number of controls are specified relating to job responsibilities, screening, terms and conditions of employment and disciplinary action. These controls are integrated with related HR policy.
- Professional codes of conduct from the BMA, GMC and NMC and others (inc Allied Health Professionals, Finance Professionals and NHS Managers).
- Research & ethics policies, including Research Governance initiatives and policy.

6. Legal & regulatory framework

The system sets out to comply with the following legal acts and the NHS regulations.

- Data Protection Act 2018
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, designs and patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Crime & Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000)
- Freedom of Information Act 2000 (re-use of public sector information regulations)

In addition to the above, other legislation can impact upon the way in which we should use information. This includes: • Children Act (1989 & 2004)

- Public Interest Disclosure Act 1998
- Audit & Internal Control Act 1987
- NHS Sexually transmitted disease regulations 2000
- National Health Service Act 1977
- Human Fertilisation & Embryology Act 1990
- Abortion Regulations 1991
- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
- Road Traffic Act 1988
- Regulations under Health & Safety at Work Act 1974

7. Accountabilities & responsibilities of key roles:

The Caldicott standard is based on the following seven principles:

- **Justify the purpose(s)** - Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
- **Don't use patient-identifiable information unless it is absolutely necessary** - Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
- **Use the minimum necessary patient-identifiable information** - Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

- **Access to patient-identifiable information should be on a strict need-to-know basis** - Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
- **Everyone with access to patient-identifiable information should be aware of their responsibilities** - Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- **Understand and comply with the law** – Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.
- **The duty to share information can be as important as the duty to protect patient confidentiality -** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

7.1 Caldicott Guardian and Information Governance Leads

Accountability for the enforcement of this policy resides with the Caldicott Guardian and Information Governance Lead for each service:

Caldicott Guardian:

Dr Kathy Ryan – Corporate Caldicott Guardian

Senior Information Risk Officer (SIRO) /Data Protection Officer(DPO): Nigel Gazzard

Data Protection Officer(DPO):

External resource Affinity Resolutions Ltd

Information Governance/Caldicott Leads for individual services:

Nigel Gazzard – Financial and Corporate Information

Dixine Douis – Broadmead Medical Centre/Homeless Health

Jane Issac – Charlotte Keep Medical Centre

Lucy Grinnell – Head of Integrated Urgent Care (IUC) Service

Sarah Pearce – Governance Manager

Deb Lowndes – Programme and Service Director

Nicki Clegg – Workforce Partner

These people also form the Information Governance Board for BrisDoc and hold the following responsibilities as detailed in their job descriptions.

The Caldicott Guardian and Information Governance Leads are expected to:

- Liaise and work with Service Managers and the NHS England/CCG in the course of promoting the Caldicott principles. They will be expected to attend various meetings as appropriate.

- To ensure standard procedures and protocols are in place to govern access to person identifiable patient and staff information.

- To ensure standard information governance procedures and protocols are in an understandable format and available to staff.

- To ensure raised awareness, through training and education, of the standards of good information governance practice and Caldicott principles, and that they are understood and adhered to.

- To work with other care providers and linked agencies to facilitate better sharing of relevant information about patients, in a manner that facilitates joined-up care across institutional boundaries while ensuring that patients' legal rights and the Caldicott Principles are maintained.

- Co-ordinate information security activities (including training) in the service ensuring staff are educated and aware of their responsibilities.
- Monitor staff compliance with policies.
- Investigate suspected and actual breaches of security and undertake reporting/remedial action as required. Maintain a log of any incidents and remedial recommendations and actions.
- Continuously assess the shortfall between both actual security measures in place and being effective and those established at a policy level thus highlighting deficiencies for remedial action.
- Establish and maintain a register of data assets for sets of information (e.g. paper files, databases) and educate the data owners on their responsibilities (what is the data, how is it used, who has access to it) (see Classifying the sensitivity of an Information Asset – Appendix 1).
- Report regularly to the IG Team on the effectiveness of information security and requesting Information Governance Team support as required when developing or amending processes for handling information.
- Contribute to decision making and carry through decisions on matters relating to security.
- Maintain an awareness of security and security enhancing technologies and brief colleagues as needed to enable measures to be implemented where and when necessary/desirable.
- Provide advice and take action, where necessary, in response to Audit findings and recommendations in respect of information security

Those responsible for personnel issues also have responsibility for:

- Linking 'change of conditions' to changes in access requirements for staff

- Linking the 'leavers' process, so that access privileges and smartcards can be revoked as soon as possible after a member of staff leaves.
- Ensuring staff are inducted on Information Governance when they commence employment.

Physical security of information and IT assets is shared across a number of areas/roles. The operation of general physical security such as door locks, entry controls will be the responsibility of all staff as it relates to all assets, not just information assets.

7.2 Senior Information Risk Officer – Nigel Gazzard

Has overall responsibility for the organisation's information risk policy. The SIRO will also lead and implement the information governance risk assessment and advise the Board on the effectiveness of risk management across the organisation.

The SIRO's responsibilities can be summarised as:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its patients
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs
- Advising the Board of Directors and or relevant accounting officer on the information risk aspects of his/her statement on internal controls
- Owning the organisation's information incident management framework

7.3 Data Protection Officer – Affinity Resolutions Ltd

The Data Protection Officer (DPO) is a role mandated for public bodies, for organisations carrying out regular and systematic monitoring of data subjects on a large scale, and for organisations carrying out large scale processing of special categories (e.g. health and social care) data or criminal convictions data. The DPO advises the organisation on data protection matters, monitors compliance and is a point of contact on data protection for the public and the ICO.

7.4 Information Asset Owner – Deb Lowndes

Information Asset Owners are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. Information Asset Owners may be assigned ownership of several assets of their organisation.

It is important to distinguish IAOs from those staff who have been assigned responsibility for day to day management of information risk on behalf of the IAOs, but are not directly accountable to the SIRO. The SIRO/IAO hierarchy identifies accountability and authority to effect change where required to mitigate identified risk.

IAOs are responsible for:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its patients

- Knowing what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset
- Knowing who has access to the asset and why, whether it be system or information to ensure access is monitored and compliant with policy
- Understanding and addressing risks to the asset, and providing assurance to the SIRO

7.5 Information Asset Assistant – All Information Governance Leads

Information Asset Assistants are usually operational members of staff who understand and are familiar with information risks in their service or operational area. Information Asset Assistants will implement the organisation's information risk policy and risk assessment process for those information assets they support and will provide assurance reports to the Information Asset Owner as necessary.

7.6 Information Security Manager - Deb Lowndes

The Information Security Manager (ISM) occupies a key role in the delivery of Information Governance activities, and the responsible individual should be tasked with providing advice on all aspects of information security and risk management, utilising either their own expertise or external advice. The quality of their assessment of information security risks, threats and advice on controls will contribute significantly to the effectiveness of the organisation's information security. For maximum effectiveness and impact the ISM should have direct access to management across the organisation and in particular to the information risk lead and IAOs or individuals with equivalent responsibilities.

The key responsibilities of the Information Security Manager are to:

- draft and/or maintain the currency of the organisation's Information Security Policy;
- ensure security accreditation of information systems in line with the organisation's approved definitions of risk;
- ensure compliance with the information security components of the IG toolkit, contributing to the annual IG assessment;
- ensure all arrangements for managing information security are effective and aligned with the organisation's Information Security and Risk Policies;
- provide reports to the senior member of management (e.g. a SIRO/IAO or equivalent) who has responsibility for Information Governance;
- provide regular information security risk assurance reports to the information risk lead (SIRO) and, depending upon the supporting structure established, to IAOs and the Information Governance Forum (or equivalent);
- co-ordinate the work of other staff with information security responsibilities;
- co-ordinate the necessary response and resolution activities following a suspected or actual security incident or breach. Keeping the information risk lead (SIRO) and information asset owners (IAO's) informed of security incidents, impacts and causes, resulting actions and learning outcomes;
- assist in the drafting of System Level Security Policies;
- assist in the development of Business Continuity Management arrangements for key information assets;

- advise in the development of a Network Security policy and controls for the secure operation of ICT networks, including remote/teleworking facilities;
- provide advice and guidance regarding the implementation of controls to mitigate against malicious or unauthorised mobile code;
- assist in designing and configuring access controls for key systems;
- assist in developing the organisation's Information Asset Register;
- develop and document an action plan for the delivery of all specific activities involving the ISM

8. Review and update of the IGMS:

The Information Governance Team will facilitate scheduled review and update of the IGMS by holding regular meetings no less than quarterly.

Review may also take place due to the following occurrences:

- Major policy breach within the company
- Identification of new threats or vulnerabilities
- Significant organisational restructuring
- Significant change in technical infrastructure
- A near miss occurrence

Some meetings may be service specific. Sub meetings may be organised and items agreed as long as the sub meeting has present at least:

- A Director of BrisDoc
- The Caldicott Lead for each service that may be affected however slightly.
- HR and IT guardians as and if appropriate.

Terms of reference for the group will be to :

- Provide advice to all staff and generally on information risk analysis/management.
- Develop, implement and enforce suitable and relevant information security policies and procedures, ensuring that these are compliant with the Data Protection Act 1998 and other legislation and regulations related to information security.
- Understand and apply the principles of confidentiality and data protection as set out in the DH publication 'Confidentiality: NHS Code of Practice, and, where current practice falls short of that required, to agree challenging and achievable improvement plans.
- Review policies and procedures on a 2 Yearly basis or as required.
- Develop and implement, together with suitable materials, an information security awareness and training programme.

- Develop and implement a comprehensive Business Continuity Planning training programme and provide advice in this area.
- Continuously assess the shortfall between both actual security measures in place and being effective and those established at a policy level thus highlighting deficiencies for remedial action.

9. Audit & compliance of information governance requirements

Staff will be made aware that routine monitoring may take place to ensure standards of service, system efficiency and appropriate use. Individuals will not be monitored without their consent, unless routine monitoring indicates a justifiable cause for concern. Such situations will have to be fully documented and relevant parties (inc legal advice, if necessary) engaged.

Audit & compliance will be carried out via a number of means:

- Spot checks on staff, review of databases and logs. Specific monitoring and review processes will be identified in each policy which relates to information governance issues.
- Annual Information Governance toolkit audit – Where applicable BrisDoc will endeavour to achieve the requirements laid out in the Information Governance toolkit to an appropriate standard as determined by the Department of Health as required for each service.
- 6 monthly review of back up and staff training logs.
- Annual review of staff employment contracts and job descriptions.
- 2 Yearly review of staff induction process.

10. Incident management – reports, investigation & disciplinary

Reporting incidents and near misses:

Any incident, near miss or potential weakness in processes, relating to the use of information, such as a breach of confidentiality or mistake due to inaccurate or unavailable information, will be reported via BrisDoc's overall 'incident reporting' and significant event analysis process.

Reporting technical/software failures:

If a user is unable to access information due to a system related issue this should be reported to the appropriate IT Manager or supplier support desk for resolution. In addition, if a system related issue puts either patient care or organisational safety at notable risk then it should also be reported via the 'incident reporting' process.

Learning from incidents:

Changes determined as a result of an incident, near miss or weakness will be cascaded across relevant staff communications as part of the process to manage the incident. This will include team briefings, newsletters. Relevant actions will be fed through to training programmes.

Investigating incident reports or concerns raised:

Any report or concern raised where the cause is unclear or misuse is suspected may be investigated further. If misuse of systems is suspected the BrisDoc IT department will be contacted at the earliest opportunity and will in conjunction with the managers above determine the need to engage specialist IT support to preserve electronic evidence. Specialist forensic IT support will be engaged in any situation where illegal activity is suspected.

Disciplinary process and removal of access rights

Any investigation, which determines that organisational policy has not been followed, maybe subject to formal disciplinary process. Access to systems for staff under investigation or disciplinary process will be suspended on the request of any senior manager involved.

Separate legal proceedings may be necessary, including seeking prosecution under the Computer Misuse Act 1990.

Where evidence is required for internal or external support of action against an individual, the processes for collection will incorporate the following standards where possible:

- Retrieval of paper information will note who withdrew it, when it was withdrawn and incorporate procedure to ensure it is not tampered with. For example the use of a medical record in investigation will record who requested and received the record, any copies of the original that were made, and who witnessed this activity.
- Electronic audit trails will be examined where possible to provide evidence. Depending on the severity of the issue specialist computer forensic support will be engaged via the Counter Fraud and Security Management Service.

11. Classifying the Sensitivity of an Information Asset

The sensitivity of an information asset relates to the type of information it contains.

Typically, the more sensitive the information is, the more restricted access will be and the greater the security that will be applied to the asset.

There are four classifications for Information Assets. These are listed in descending order of sensitivity below:

(i) Confidential

This includes any data that contains personal details about a service user, customer, donor, volunteer or staff member. It also includes financial data such as credit card and bank account details.

Unauthorised disclosure of this type of data may:

- Threaten the safety or security of an individual.
- Damage the public’s trust in BrisDoc.

- Have a significant impact on the organisation’s voluntary income.
- Result in substantial financial penalties being imposed on BrisDoc.
- Result in the loss of service contracts and damage the organisation’s ability to win more contracts.
- Expose BrisDoc to legislative or regulatory penalties or sanctions.

(ii) Restricted

- This includes service development plans, detailed financial information, consolidated salary data, systems access details. Typically this data will be restricted to certain members of staff, e.g. salary data will only be accessible by the payroll team, HR and a person’s line manager.
- Unauthorised disclosure of this type of data may:
- Threaten the security of other information assets.
- Have a detrimental impact on income generation activities.
- Provide a competing organisation with a competitive advantage.
- Result in embarrassment to BrisDoc.

(iii) Internal Only

- This is information that must only be viewed by staff, volunteers, trustees and selected third parties. Examples of data in this classification would include processes and procedures used by the organisation, internal staff directories and “know how” that may be useful to a competing organisation.
- Unauthorised disclosure of this type of data may:
- Cause minor embarrassment to BrisDoc.
- Provide competing organisations with BrisDoc “know how” which they could use to their advantage.

(iv) Public

- This information can be distributed in the public domain. Examples of information in this classification is information that is widely distributed in the public domain such as, public facing web sites, financial reports required by regulators, newsletters for external distribution, or press releases.

- Where a person is uncertain of the classification of an Information Asset they should seek advice and consult with the service manager that has authority to view that information. Where doubt still remains the asset must be classified at the highest level that they think the asset requires.
- Where an Information Asset has different levels of information the asset must be classified using the most sensitive classification. As an example, if a business plan included reference to a bank account then the asset would be classified as Confidential.

Change Register

Tables

Date	Vn	Author	Comments
23/11/10	001	D Douis	
26/11/10	1.1	D Douis	Revised after review
07/01/11	1.2	D Douis	Revised after IG meeting
12/14/11	1.3	Deb Lowndes	Clarification of Caldicott principles in sec 7. Re-structuring of sec 3 to differentiate between BrisDoc IG System and additional reference documents
12/1/12	1.3.2	Deb Lowndes	Amendments after review by CB & DD
29/6/12	1.3.3	Deb Lowndes	Addition of SIRO/IAO/ISM Roles
24/7/12	1..3.4	Deb Lowndes	Review by CB/NG and subsequent sign-off by NG
12/11/12	1.3.5	Deb Lowndes	Additional documents added
09/09/13	1.3.6	Deb Lowndes	Amendments to reflect new organization structure and addition of Corporate Governance Document reference
26/06/14	1.3.7	Deb Lowndes	Amendments to reflect new organization structure and amendments to reflect documents held.
14/07/15	1.3.8	Deb Lowndes	Amendments to include social media policy, Data Sharing with 3rd Parties Pseudonymisation & Anonymisation Policy new policy and new service GPST
01/03/15	1.3.9	Deb Lowndes	Update KR and KB details
21/06/16	1.3.10	Deb Lowndes	Annual review
17/12/18	2.0	Deb Lowndes	Annual Review and Changes for GDPR
28/01/20	2.1	Deb Lowndes	Annual Review
18/01/20	2.2	Deb Lowndes	Annual Review
15/03/22	2.3	Deb Lowndes	Annual Review
20/03/24	2.4	Deb Lowndes	Annual Review