BrisDoc Patient care by people who care

Proudly employee owned.

Information Governance Framework

Version:	Owner:	Created:
2.6	Jon Rex (Head of DDaT)	October 2026
Published:	**Approving Director:**	**Next Review**
17/04/2025	Rhys Hancock (Director of Nursing, AHPs and Governance)	17/04/2027

Contents

Purpose & Principles **5**
Scope **5**
BrisDoc's Information Governance Management System (IGMS) **6**
Main Policies *6*
Access to Health Records *6*
Data Protection by Design Policy *6*
Data Protection Policy *6*
Data Protection, Confidentiality & Disclosure Policy *6*
Data Sharing with 3rd Parties Pseudonymisation and Anonymisation Policy *6*
Email Operational Guidance *6*
Information Security *7*
Mobile Computing *7*
Monitoring Access to Patient Information *7*
Network Security *7*
Records Management *7*
Smartcard Policy & Smartcard Practice Services *7*
Social Media Policy *7*
Co-owners Information Governance Awareness and Training *8*
Related Policies, Procedures and Resources *8*
Corporate Governance Framework *8*
Data Flow Mapping & Information Asset Register *8*
Business Continuity/Disaster Recovery *8*
Third Party Confidentiality Agreement *8*
Learning Event Policy *9*
Data Breach Notification Procedure *9*
Press and Media Policy *9*
Co-owners Awareness and Training **9**
Induction Process *9*
Annual Training *9*
Additional Roles *9*

Other Related Policy & Code(s) of Practice 9
Legal & Regulatory Framework **9**
Legislation 10
Data Protection and Privacy 10
Health and Social Care Specific Laws 10
Cybersecurity and IT Regulations 10
Regulatory and Professional Standards 10
NHS and Government Policies 10
National Regulators and Oversight Bodies 10
Ethical and Best Practice Guidelines 10
Accountabilities & Responsibilities of Key Roles **11**
Information Governance Leads 11
Governance & Compliance 12
Training & Awareness 12
Data Management & Security 12
Leadership & Decision-Making 12
Senior Information Risk Officer – Debs Lowndes 12
Caldicott Guardian – Dr Kathy Ryan 13
Data Protection Officer – Regulatory Solution Ltd 13
Information Asset Owner – All Information Governance Leads 14
Information Asset Assistant – as delegated by IAO's 14
Information Security Manager - Deb Lowndes 14
Policy & Compliance 14
Risk Management & Reporting 15
Technical & Operational Support 15
Strategic Planning & Development 15
Review and Update of the IGMS **15**
Audit & Compliance **16**
Incident Management – reports, investigation & disciplinary **16**
Reporting incidents and near misses 16
Reporting technical/software failures 16
Learning from Events 16
Investigating Incident Reports or Concerns Raised 16
Disciplinary Process and Removal of Access Rights 17

Classifying the Sensitivity of an Information Asset 17

Confidential 17

Restricted 17

Internal Only 18

Public 18

Change Register 18

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 co-owners are equipped to manage 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.

Co-owners are responsible for:

- Maintaining physical security of the building whilst on duty.
- Always maintaining security of identifiable information.
- 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 Information Governance Leads via BrisDoc's incident Portal.

Scope

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

- Patient/Client/Service User/Citizen information
- Co-owner related information
- Organisational information

The IGMS covers all aspects of managing 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
- Co-owners conduct relating to the use of information in any form

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

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:

Main Policies

Access to Health Records

Where available: Company intranet.

The purpose of this document is to detail the process and responsibilities for dealing with patient requests to personal information within BrisDoc's Patient Services.

Data Protection by Design Policy

Where available Company intranet.

The document covers procedures to be adopted when any significant change or addition is made to BrisDoc's information assets and systems, including operating systems, application systems, hardware and data collection systems and clinical changes which impact on activity.

Data Protection Policy

Where available Company intranet.

This Data Protection Policy sets out how BrisDoc Healthcare Services Ltd "the Organisation" manages the Personal Data of our patients, suppliers, co-owners, workers and other third parties.

This Data Protection Policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present co-owners, workers, patients or supplier contacts, website users or any other Data Subject.

This Data Protection Policy applies to all co-owners.

Data Protection, Confidentiality & Disclosure Policy

Where available: Company intranet.

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.

Data Sharing with 3rd Parties Pseudonymisation and Anonymisation Policy

Where available: Company intranet.

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. ICBs and universities/health bodies for research purposes.

Email Operational Guidance

Where available: Company intranet.

This document provides operational guidance on email usage, outlining responsibilities and legal requirements. It covers the handling of patient/person-identifiable, corporate, and sensitive data when sending emails.

Information Security

Where available: Company intranet.

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.

Mobile Computing

Where available: Company intranet, shared drives at bases.

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

Monitoring Access to Patient Information

Where available: Company intranet.

The purpose of this document the detail the confidentiality audit procedures that apply within BrisDoc's Services.

Network Security

Where available: Company intranet.

The purpose of this document is to describe the Network Security Policy that applies within BrisDoc. 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.

Records Management

Where available: Company intranet.

The policy supports the effective creation, use, storage, and disposal of records in compliance with legal, regulatory, and best practice standards. Its primary purpose is to support high-quality patient care, ensure data accuracy and accessibility, and maintain confidentiality and security in line with the Data Protection Act 2018, UK GDPR, and the Records Management Code of Practice for Health and Social Care 2021. The policy establishes clear responsibilities for co-owners managing records throughout their lifecycle, ensuring information is retained appropriately and disposed of securely when no longer needed.

Smartcard Policy & Smartcard Practice Services

Where available: Company intranet.

The purpose of these Smartcard Policies 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.

Social Media Policy

Where available: Company intranet.

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

Co-owners Information Governance Awareness and Training

Where available Company intranet.

This document focuses on how co-owners 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 co-owners.

Related Policies, Procedures and Resources

Corporate Governance Framework

Where available: Company intranet.

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.

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 Information Asset Owners (IAO) in conjunction with the Information Asset Administrator (IAA).

Business Continuity/Disaster Recovery

Where available: Company intranet.

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. A related policy is the Major Critical Incident Policy.

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, co-owners 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 as defined within their contract.

They could include the following:

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

Learning Event Policy

Where available: Company intranet.

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

Data Breach Notification Procedure

Where available: Company intranet.

The document sets out the data breach notification procedure. Data Breach Notification Procedure

Press and Media Policy

Where available: Company intranet.

The document sets out the approach to press and media, about media and press enquiries and a draft cyber press release.

Co-owners Awareness and Training

Induction Process

As part of induction all co-owners are made aware of the following.

- IG Handbook that sets out IG and co-owner role specific advice
- General awareness of the Caldicott Principles
- General awareness of the social media and IT systems safety.

Annual Training

All co-owners are required to complete e-Learning for Healthcare Data Security Awareness Level 1 annually.

The People Team track completion for submission for the annual Data Protection Security Toolkit Assessment.

Additional Roles

The SIRO and CG complete additional training supplied by third parties.

Other Related Policy & Code(s) of Practice

- Workforce Policies – In setting out standards relating to Information Governance several controls are specified relating to job responsibilities, screening, terms and conditions of employment and disciplinary action. These controls are integrated with related People 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.

Legal & Regulatory Framework

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

Legislation

Data Protection and Privacy

- **UK General Data Protection Regulation (UK GDPR)** – Governs the processing of personal data, ensuring legal, fair, and transparent use.
- **Data Protection Act 2018 (DPA 2018)** – Supplements UK GDPR, setting additional provisions for healthcare data, including exemptions and rights.
- **Human Rights Act 1998** – Article 8 ensures the right to respect for private and family life, impacting data confidentiality.
- **Freedom of Information Act 2000 (FOIA)** – Grants public access to information held by public authorities, subject to exemptions.

Health and Social Care Specific Laws

- **Health and Social Care Act 2012** – Introduced key governance responsibilities, including data sharing for care provision and research.
- **Access to Health Records Act 1990** – Regulates access to a deceased person's health records.
- **Children Act 1989 & 2004** – Outlines data-sharing duties for child safeguarding.
- **Mental Capacity Act 2005** – Includes guidance on handling data for individuals lacking capacity.

Cybersecurity and IT Regulations

- **Network and Information Systems (NIS) Regulations 2018** – Ensures cybersecurity resilience for critical services, including the NHS.
- **Computer Misuse Act 1990** – Addresses unauthorised access and misuse of NHS systems.

Regulatory and Professional Standards

NHS and Government Policies

- **NHS Code of Practice on Confidentiality** – Provides principles for handling patient-identifiable data.
- **NHS Digital's Data Security and Protection Toolkit (DSPT)** – Requires annual assessment of IG compliance.
- **Caldicott Principles** – Govern the ethical and legal use of patient-identifiable information.
- **Records Management Code of Practice for Health and Social Care (2021)** – Defines NHS records management responsibilities.

National Regulators and Oversight Bodies

- **Information Commissioner's Office (ICO)** – Regulates data protection and privacy compliance.
- **National Data Guardian (NDG)** – Provides independent advice on data security and privacy matters.
- **Care Quality Commission (CQC)** – Ensures patient data security as part of overall healthcare quality assessments.

Ethical and Best Practice Guidelines

- **General Medical Council (GMC) Guidance on Confidentiality** – Provides standards for patient data handling by medical professionals.
- **National Cyber Security Centre (NCSC) Guidance** – Offers best practices for cybersecurity risk management.

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 co-owners - 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.
- **Inform patients and service users about how their confidential information is used -** A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this.

Information Governance Leads

Accountability for the enforcement of this policy resides with the Senior Information Risk Officer (SIRO), Caldicott Guardian (CG), Data Protection Officer (DPO) and Information Governance Lead for each service/function.

- Information Governance Leads for individual services/functions:
  - Peter Richardson – Finance
  - Diane Douglas – Broadmead Medical Centre/Homeless Health
  - Diane Douglas – Charlotte Keep Medical Centre
  - Lucy Grinnell – Head of Integrated Urgent Care (IUC) Service, Facilities, Rota
  - Sarah Pearce – Governance Manager
  - Karen Miller – People Partner

The above form the Information Governance Board with the SIRO and CG, for which the board terms of reference determine their roles.

Information Governance Leads are responsible for ensuring compliance with information governance policies and maintaining high standards of data security. Their key responsibilities include:

Governance & Compliance

- Collaborate with the SIRO, DPO, and Caldicott Guardian to maintain and implement the Information Governance Management System (IGMS).
- Ensure policies and procedures governing access to patient and co-owner identifiable information are in place and adhered to.
- Monitor compliance with information governance policies and procedures, ensuring staff understand and apply them correctly.
- Investigate security breaches, report incidents, and take remedial action. Maintain a log of incidents and follow up on recommendations.
- Conduct regular assessments to identify gaps between policy requirements and actual security measures, addressing deficiencies.

Training & Awareness

- Promote awareness of good information governance practices and Caldicott Principles through training and education.
- Ensure staff are provided with clear guidance, resources, and training on information governance policies.
- Coordinate information security activities, including training, to ensure co-owners understand their responsibilities.

Data Management & Security

- Work with care providers and external agencies to facilitate secure and compliant information sharing that supports joined-up care.
- Maintain a data asset register, ensuring owners understand what data they hold, how it is used, and who has access.
- Stay informed on security-enhancing technologies, implementing necessary measures and briefing colleagues on relevant updates.

Leadership & Decision-Making

- Attend the IG Board and contribute to decision-making on information security matters.
- Implement and act on audit findings to improve information security and governance processes.

Those responsible for personnel issues also have responsibility for:

- Linking ‘change of conditions’ to changes in access requirements for co-owners.
- Linking the ‘leavers’ process, so that access privileges and smartcards can be revoked as soon as possible after a co-owner leaves.
- Ensuring co-owners are inducted on Information Governance when they commence employment.

Senior Information Risk Officer – Debs Lowndes

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:

- The Senior Information Risk Owner (SIRO) should be an Executive Director or other senior member of the board (or equivalent senior management group/committee). The SIRO may also be the Chief Information Officer (CIO) if the latter is on the board but should not be the Caldicott Guardian, as the SIRO should be part of the organisation's management hierarchy rather than being in an advisory role.
- The SIRO will be expected to understand how the strategic business goals of the organisation may be impacted by information risks, and it may therefore be logical for this role to be assigned to a board member already leading on risk management or information governance.
- The SIRO will act as an advocate for information risk on the board and in internal discussions and will provide written advice to the Chief Executive Officer (CEO) on an annual basis in regard to information risk aligned to the Data Protection Security Toolkit (DPST) submission.
- The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed and should have ownership of the Information Risk Policy and associated risk management strategy and processes. He / she will provide leadership and guidance to a number of Information Asset Owners.

The key responsibilities of the SIRO are to:

- Oversee the development of an Information Risk Policy, and a strategy for implementing the policy within the existing Information Governance framework.
- Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk
- Review and agree action in respect of identified information risks.
- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment, and execution and that this is communicated to all co-owners.
- Provide a focal point for the resolution and / or discussion of information risk issues.
- Ensure the board is adequately briefed on information risk issues.
- Ensure that all care systems information assets have an assigned Information Asset Owner.

Caldicott Guardian – Dr Kathy Ryan

The Caldicott Guardian is responsible for ensuring the ethical and lawful use of patient and co-owners' information in BrisDoc. Their primary role is to uphold Caldicott Principles, which guide the appropriate sharing and protection of confidential data. They oversee information governance policies, advise on data-sharing decisions, and ensure compliance with legal frameworks such as the UK Data Protection Act and GDPR. Caldicott Guardians work closely with senior management, Information Governance leads, and clinicians to balance patient and co-owners' confidentiality with the need for appropriate data access in healthcare delivery. Their role is crucial in safeguarding patient trust while enabling effective care and service planning.

Data Protection Officer – Regulatory Solution 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.

Information Asset Owner – All Information Governance Leads

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 co-owners 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

Information Asset Assistant – as delegated by IAO's

Information Asset Assistants are usually operational members of co-owners 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.

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 to the information risk lead and IAOs or individuals with equivalent responsibilities.

The Information Security Manager (ISM) plays a critical role in safeguarding the organisation's information security. Their key responsibilities include:

Policy & Compliance

- Develop and maintain the Information Security Policy, ensuring it remains up to date.
- Oversee the security accreditation of information systems in line with the organisation's risk framework.
- Ensure compliance with information security standards outlined in the IG Toolkit and contribute to the annual IG assessment.
- Align all security management arrangements with the organisation's Information Security and Risk Policies.

Risk Management & Reporting

- Provide regular security risk assurance reports to the Senior Information Risk Owner (SIRO) and relevant governance bodies.
- Investigate and coordinate responses to security incidents or breaches, ensuring SIRO and Information Asset Owners (IAOs) are informed of risks, impacts, and actions taken.
- Lead and coordinate the work of staff responsible for information security across the organisation.

Technical & Operational Support

- Assist in drafting System Level Security Policies to strengthen organisational security measures.
- Support the development of Business Continuity Management plans for key information assets.
- Contribute to the creation of a Network Security Policy, ensuring secure ICT operations, including remote/teleworking facilities.
- Provide expert guidance on access controls, malware protection, and security measures for key systems.

Strategic Planning & Development

- Assist in developing and maintaining the Information Asset Register to track and manage data security.
- Create and document an action plan to oversee and execute security-related activities effectively.

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 annually.

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 if the sub meeting has present at least:

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

Terms of reference for the group will be to:

- Provide advice to all co-owners 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 all references in Section 6 of this document.

- 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.

Audit & Compliance

Co-owners 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 conducted via a number of means:

- Spot checks on co-owners, 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 reviews of back up and co-owners training logs.
- Annual review of co-owners' employment contracts and job descriptions.
- 2 Yearly reviews of co-owners' induction process.

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 'learning event' 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 Events

Changes determined because of an incident, near miss or weakness will be cascaded across relevant co-owners' 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 co-owners 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.

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:

Confidential

This includes any data that contains personal details about a service user, customer, donor, volunteer, or co-owner's 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.

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 co-owners, 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.

Internal Only

- This is information that must only be viewed by co-owners, volunteers, trustees and selected third parties. Examples of data in this classification would include processes and procedures used by the organisation, internal co-owners' 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.

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 remains the asset must be classified at the highest level that they think the asset requires.
- Where an Information Asset has various 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

Date	Vn	Author	Comments
23/11/10	1.0	D Douis	Initial Document
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
21/01/25	2.5	Deb Lowndes	Annual Review and Change of SIRO, with review by DPO.
29/10/2026	2.6	Jon Rex	IG Lead Names updated