

Patient Care By People Who Care

INFORMATION ASSET AND SYSTEM CHANGE NOTIFICATION POLICY AND PROCEDURE

Created: October 2012

Created by: Deb Lowndes

Job Title: IT Manager

Version: 2.7

Review: November 2022

Reviewed on: November 2020

Reviewed by

Name: Sarah Pearce

Job Title: Patient Safety and Compliance Coordinator

Signed by Director

Name: Nigel Gazzard

Signature:



Job Title: Managing Director

Document control

| June-12 | 1.0 | DL | First Draft |
|---------------|-----|-------|---|
| October-12 | 1.1 | DL | Formatting and amendments after first review |
| September 14 | 2 | SP | Reviewed – Amended job titles |
| September 16 | 2.1 | DL | Annual review |
| July 2017 | 2.2 | DL | Addition of NHS Vulnerability Assessment Good Practice for infrastructure assessment |
| December 17 | 2.3 | DL | Addition of Equality Impact Screening Matrix |
| April 2018 | 2.5 | DL | Update of PIA template |
| November 2018 | 2.6 | SP/DL | Routine review and to reflect reference to new DPST and refinement of PIA questions as a result of revised ICO template |
| Oct-2020 | 2.7 | DL | Version reviewed – No amendments |

CONTENTS

| | |
|---|----|
| 1. Introduction | 3 |
| 2. Scope of the Procedure | 3 |
| 3. Purpose of the Procedure | 4 |
| 4. Responsibilities | 4 |
| 5. Record Keeping And Auditing Of Changes To Systems | 5 |
| 6. Procedure Awareness | 5 |
| 7. Privacy assessment | 5 |
| 8. Monitoring and Control | 5 |
| Appendix A –Notification of the Development of a New Information System or Change to an Existing System. | 6 |
| APPENDIX B – (IG Checklist) Areas to be considered when introducing new, or changing existing systems | 7 |
| Appendix C - Privacy Impact Assessment Template | 10 |
| Appendix D - Equality Impact Screening Matrix | 22 |

1. INTRODUCTION

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of BrisDoc.

This procedure outlines the standards used for the testing of software and hardware, which is used at BrisDoc.

An essential requirement for any change management control system is the establishment of 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. It is vitally important that all such assets have identified Information Asset Owners (IAO) who are responsible for maintaining appropriate standards of confidentiality, integrity, and accessibility and ensuring that data quality is not adversely affected by any changes. IAOs are responsible for any inward and outward flows, managing risks and ensuring that any new systems or changes to systems are assessed for privacy compliance prior to implementation.

In order to adhere to good practice for the management of information assets this document establishes a formal mechanism for the approval of new assets and potential changes to existing assets and processes. This will ensure that any security, confidentiality, data protection and data quality issues have been considered for any new or re-configured asset, system or procedure.

By completing the Change Notification Form (Appendix A) and completing the Information Governance (IG) Checklist (Appendix B) an initial compliance assessment of privacy risks and liabilities will then have been conducted. The need for a more detailed Privacy Impact Assessment (PIA) can then be made.

2. SCOPE OF THE PROCEDURE

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

The policy applies to all members of staff (including consultant, contract, agency) engaged by BrisDoc.

The policy covers changes which will have an effect on information systems (paper and electronic) which could include installing a brand-new system (hardware/software), replacing an existing system or upgrading operating systems, or a significant change to collection processes. An example of a major change would be the introduction of a new data warehouse, introducing a new GP portal to an existing warehouse, commissioning an external company to provide a service or process data on behalf of BrisDoc.

3. PURPOSE OF THE PROCEDURE

The purpose of the procedure is to ensure that any changes to services are communicated and managed and consideration has been made to compliance with confidentiality, data protection and data quality requirements.

The document sets out a simple, but formal, process that requires managers and project managers to notify intended changes to the Information Governance Board, through the completion of the Change Notification Form (Appendix A). The process then requires the manager responsible for system implementation to assess any significant gaps by completing the IG Checklist See Appendix B. This will reveal the areas for further work or development.

The initial assessment of privacy risks and liabilities will indicate whether a Privacy Impact Assessment (PIA) is required. PIA is a process which helps assess privacy risks in the collection, use and disclosure of information. They are recommended where new and intrusive technology is used or where private or sensitive information which was originally collected for a limited purpose is going to be re-used in a new and unexpected way. Guidance is provided in the PIA handbook produced by the Information Commissioner's Office (ICO).

4. RESPONSIBILITIES

All staff need to work together to help identify and mitigate information risk. Managing information risk effectively requires a structured approach involving work areas where accountability sits with business managers, rather than specialist staff.

4.1 The **Senior Information Risk Owner (SIRO)** has ownership of the organisation's information risks and provides assurances to the Board. The SIRO is responsible for assessing the risks associated with changes to existing systems or the development of new information systems and for providing final approval.

4.2 The **Information Governance Board (IGB)** must be consulted during the design phase of any new service, process or information asset and be made aware of any risks associated with the development. They will formally approve any IG components of the development, including the PIA. This will ensure that the SIRO can provide the necessary assurances to the Board.

4.3 The **Information Asset Owners (IAO)** are accountable for the information systems under their control and are responsible for managing the risks associated with any data flows into and out of those systems and for the quality, security and confidentiality of any data held in them.

4.4 It is important that the following roles are consulted when planning change as they offer the best knowledge of a planned, new or existing information asset, its intended purposes and its operating environments. It is therefore important that:

The **Information Governance Board** should be involved to ensure compliance with confidentiality and data protection issues. They will consult and seek approval from the Caldicott Guardian regarding the exchange and use of personally identifiable data and the need for Information Sharing Agreements if appropriate.

The **Performance and Information Analyst** should be involved to ensure account is taken of potential impacts on the integrity and quality of the information.

The **Head of Business Information and projects** should be involved at an early stage in the development of new or re-configured electronic systems to ensure the selected security controls are identified, implemented properly and tested.

4.5 All staff members who may be responsible for introducing changes to services, processes or information assets must be informed effectively about the requirement to seek approval from the group that considers information governance compliance issues.

5. RECORD KEEPING AND AUDITING OF CHANGES TO SYSTEMS

An audit trail will be kept. Each change will have a form which will record progress at every stage. The form will be the basis of the final implementation change control decision process.

6. PROCEDURE AWARENESS

It will be the responsibility of the Information Governance Board to make sure that all relevant managers are aware of the procedure, explain its implications and ensure that it is made available on the intranet and shared drives as appropriate.

7. PRIVACY ASSESSMENT

Privacy impact assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. PIAs are an integral part of taking a privacy by design approach.

8. MONITORING AND CONTROL

The Information Governance Board will monitor the introduction of new services and the compliance with the procedure. Failure to use the procedure will be recorded and appropriate follow-up action taken.

APPENDIX A – NOTIFICATION OF THE DEVELOPMENT OF A NEW INFORMATION SYSTEM OR CHANGE TO AN EXISTING SYSTEM.

Please complete this form, if you are proposing to introduce a new information hardware, software or paper system, or re-develop an existing system.

| |
|---|
| 1. Please provide a description of the system proposed. (This should include whether it is an operational or commissioning system, whether a Data Warehouse or Reporting system). |
| 2. Please state the likely implementation date. Date: |
| 3. Please list the information that you intend to process, store or intend to collect (aggregated, if personal or sensitive, list e.g. name, address, date of birth, NHS Number, diagnosis, attendance date etc). |
| 4. Please state the source or sources of the data imported? (e.g. SUS, PDS, GP systems). |
| 5. Please list the users of the system/data and any intended recipients of data? (e.g. Commissioners, CCG's, GPs Surgery, Clinicians etc). |
| 6. What other systems will it be connected to? (Corporate, GP, none). |
| 7. Who will be the system Information Asset Owner? Name _____ Title _____ |
| 8. Who will be the Information Asset Administrator? Name _____ Title _____ |
| 9. Who will control access to the system? Role _____ Name _____ Title _____ |
| 10.10 How will access to the system be controlled? (smartcard, password, Role Based Access) . |
| 11.11 Where will the system be located/housed? Location _____ |
| 12. Who will develop and support the system? (e.g. internal/external company) |
| 13. Please state potential risks associated with the introduction of this system/change. (e.g. security, confidentiality) |

APPENDIX B – (IG CHECKLIST) AREAS TO BE CONSIDERED WHEN INTRODUCING NEW, OR CHANGING EXISTING SYSTEMS

| Area for consideration | Yes/No | Further work needed | Reference document /IGT/Internal/External |
|--|---------------|---|---|
| A – General | | | |
| A1 | New or Change | Have the Information Governance Board been informed of the planned new/changed system or process? | Terms of Reference of Information Governance Board |
| A2 | New | Has staff accessing the information system undertaken appropriate information governance training? | Mandatory Training Policy |
| B - Confidentiality/Data Protection | | | |
| B1 | New or Change | Has the 'data controller' status been clearly identified? | Data Protection Policy |
| B2 | New or Change | Does the system contain data that would be subject to Subject Access/Access to Health Records requests? | Subject Access Request Policy Freedom of Information Policy |
| B3 | New | Will protocols be required to govern the sharing of information with other agencies or partners? | Information Governance Toolkit Requirement 9-207, Information Sharing Protocol. |
| B4 | New | If required are there processes in place to obtain patient/service user consent for holding/sharing their information? | Code of Confidentiality Policy |
| B5 | New | Are processes in place to inform patients/service users how their information will be used at the time they are asked to provide it? | Code of Confidentiality Policy |
| C Data Quality | | | |
| C1 | New or Change | Will change impact on the quality of the data e.g. its completeness, accuracy, relevance, accessibility, | Data Quality Policy |
| C2 | New | Does the system have the ability to record and verify the NHS number? | Use of NHS # Project action plan |
| C3 | New | Has consideration been given to methods of data reconciliation and validation? | Data Quality Policy |
| C4 | New | Are national or locally defined data standards being used wherever possible? | Data Quality Policy |
| C5 | New | Where different systems are recording the same data, are processes in place to ensure there are no inconsistencies between them? | Data Quality Policy |
| C6 | New | Can changes to records be tracked to identify who has made the change i.e. audit trail in electronic system, signed changes in paper records? | Data Quality Policy/ Information Security Policy |

| D | | Information Security | |
|----------|----------------|--|--|
| D1 | New | Are relevant security systems in place to ensure that identifiable information is protected from unlawful or unauthorised access e.g. appropriate access controls? | Information Security Policy |
| D2 | New | Have processes been considered to protect information from accidental loss, destruction or damage? | Information Security Policy |
| D3 | New | Are controls in place to physically protect assets and ensure availability of utilities and services? | Information Security Policy |
| D4 | New | Are controls in place to protect the system/network from malicious software? | Information Security Policy |
| D5 | New | Are backup processes in place, or will they be developed? | Information Security Policy |
| D6 | New | If data is transferred, are security methods in place to ensure secure transfer of routine information flows? | Information Security Policy / Transfer of Personal or Business Sensitive Information |
| D7 | New | Are access controls in place | Information Security Policy, Access Control Policy |
| E | | Records Management | |
| E1 | New or /Change | Will changes/introduction of new system impact on the ability to dispose, retain or archive information appropriately? | Records Management Policy Retention & Disposal Schedules |
| E2 | New | Is there an agreed retention/destruction period (based on local agreement or legal minimum retention periods)? | Records Management Policy and associated procedures |
| F | | Freedom of Information | |
| F1 | New/Change | Does the system contain information which may be subject to Freedom of Information requests? | Freedom of Information Policy and Procedure |

Infrastructure Vulnerability Assessments

The purpose of an Infrastructure vulnerability assessment is to ensure that any significant new infrastructure is installed in an appropriately secure manner or that when existing infrastructure undergoes a significant change that vulnerabilities are not introduced. Infrastructure includes servers, switches, routers, databases, firewalls, etc.

Infrastructure vulnerability assessments should be scoped individually; each may include, but are not limited to the following elements:

- Network vulnerability scanning.
- Manual testing.
- On-host auditing.
- Web server scanning.
- Basic database checks.

| Proposed Change | Infrastructure Assessment | Application Assessment |
|---|---------------------------|------------------------|
| New network connection to the Internet | Yes | No |
| New infrastructure on existing connections to the Internet | Yes | No |
| New network connection to NHS network | Yes | Check |
| New infrastructure on existing connections to NHS network | Yes | Check |
| New network connection to commercial network | Yes | No |
| New infrastructure on existing connections to commercial network | Yes | No |
| New network connection to the PSN | Yes | No |
| New infrastructure on existing connections to the PSN | Yes | No |
| New network connection to other government network | Check | No |
| New dial in connection from 3 rd party supplier | Check | No |
| New remote incoming connections from the organisations users | Check | Check |
| Changed registration, authentication or authorisation process over Internet | No | Yes |
| Changed registration, authentication or authorisation process over NHS network | No | Yes |
| Changed registration, authentication or authorisation process over PSN | No | Yes |
| Changed registration, authentication or authorisation process over other Government network | No | Check |
| Additional instances of existing servers | Check | No |
| Operating system or infrastructure upgrades | Check | Check |
| New or substantially changed application service | No | Yes |
| Substantial changes to infrastructure software or configuration | Yes | Yes |
| Interface changes for the organisations systems with data above OFFICIAL | Yes | Yes |
| New organisation systems data above OFFICIAL | Yes | Yes |
| Financial transactions with remote Organisations | Check | Check |
| New or changed internal access control infrastructure | Check | Check |

APPENDIX C - PRIVACY IMPACT ASSESSMENT TEMPLATE

Section A: Introduction

The privacy impact assessment (PIA) is a tool to help ensure we manage the risk of data breaches or the other inappropriate use of data that could cause patient distress and have a reputational or financial impact to BrisDoc CCG.

It is designed to help staff ensure they carefully consider what data they need, and how they will manage it.

To complete the PIA fill in sections B and C, and get sign off using section D.

To help you complete the PIA you should read BrisDoc's policies and guidance on information governance and security, which are available on radar.

You can also get advice from BrisDoc's IG lead, Caldicott Guardian, or Senior Information Risk Officer

You can use this template to review an existing piece of work, but you might find it helpful to do a privacy audit of on-going work that has not had a PIA.

However, a PIA **must** be done for new projects or data flows, or for projects or whose data uses are being changed in any way.

When completing your PIA please ensure it is as detailed as possible. You might find it helpful and easier to attach supporting evidence, which you may do instead of completing the narrative boxes in the template.

The PIA can be signed off by the IG lead, Caldicott Guardian, or Senior Information Risk Officer. This will be reported to the IG Board.

When completed a signed copy of the PIA should be kept with your project documentation and a copy provided to the Information Governance Lead.

Section B: The Project

This section needs details of the project or programme you are working on, the kind of data you are seeking, and the route by which you may access it. Information Governance is in **Section C**.

1. Describe the data do you want to use and the system or projects for which data are being/to be used. Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. Include how many individuals are likely to be affected by the project. What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What measures do you take to ensure processors comply?

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the PIA process.

Risks and Solutions

Identify the key privacy risks and the associated compliance and corporate risks. Describe the actions you could take to reduce the risks, and any future steps which would be necessary. Provide an assessment of whether the risk is eliminated, reduced or accepted.

[Go to Question 2](#)

2. Will the data contain patient identifiers such as name, record number etc?

| | | |
|-------------------------------------|--------------------------|--------------------|
| A Yes: NHSNumber/Postcode | <input type="checkbox"/> | Go to Question 3 |
| B Yes: but more data than A | <input type="checkbox"/> | Go to Question 3 |
| C: No the data are anonymous | <input type="checkbox"/> | Go to Paragraph 10 |

3. Good information governance requires anyone proposing to use data to try and get patient consent or to use anonymised data.

| | |
|---|--------------------------|
| A Check this box if it is impractical to obtain explicit consent | <input type="checkbox"/> |
| A Check this box if it is impractical to use anonymous data | <input type="checkbox"/> |

Explain why, below

Go to Question 4

4. What is the basis for accessing and processing the data or information you need?

| | | |
|-----------------------------|--------------------------|------------------|
| A Direct Consent | <input type="checkbox"/> | Go to Question 5 |
| B Implied Consent | <input type="checkbox"/> | Go to Question 6 |
| C Exemption e.g. ASH | <input type="checkbox"/> | Go to Question 5 |
| D Another basis | <input type="checkbox"/> | Go to Question 7 |

- 5. Please attach supporting evidence to this PIA and/or describe in the box below how consent is obtained. Alternatively explain how e.g. ASH status would be applicable.

You have finished this Section.

Now complete **Section C**

- 6. Describe how the standard for implied consent is met: who has the relationship with the patient; have any capacity issues been addressed; and how are you assured the patient has had an opportunity to object to this use of their data?

You have finished this Section.

Now complete **Section C**

- 7. What is the other basis that you have identified?

A Public Health Regulations

Go to Question 8

B Court order/regulatory power

Go to Question 8

C Overriding public

Go to Question 8

C None /unknown

Go to Paragraph 9

8. Please provide details or attach supporting evidence ; or detail how the having the data or information required is in the overriding public interest.

You have finished this Section.

Now complete **Section C**

9. On the basis of the information provided:

As there is no known basis for you to access the data you are seeking your PIA would not be signed off. You should not continue completing this form. Please speak to the information governance lead or your manager about how to proceed.

10. On the basis of the information provided:

It looks as if you do not need to complete a PIA. You should not continue completing this form. Do you need to do an **Equality Impact Assessment**? Please speak to your manager about how to proceed.

End of Section B

Section C: Information Governance and Privacy Impact

By completing this section you are providing assurance that your use of data is compliant with overarching requirements, mainly the Caldicott Principles and the Data Protection Act.

1. How will the data/information be obtained?

2. How will the data or information obtained be limited to what is required?

3. How and where will the data or information be stored? How much data?

4. When is it proposed the data or information will no longer be needed? What is the required retention period?

5. Who is the controller of the data or information at BrisDoc ? Who will have access to it?

6. On the basis of the answers you have given to Sections B and/or C please describe what privacy impacts you have identified and how these will be mitigated.

You have finished this Section.

Now complete **Section D**

End of Section C

Section D: Approval

The author should complete questions 1 to 4. A person from Information Governance should complete question 5. The person signing off the PIA should complete questions 6

1. I confirm that **all** the people involved in handling the information or data discussed in this document have:

| | |
|---|--------------------------|
| A Understood CCG policies on Information Governance | <input type="checkbox"/> |
|---|--------------------------|

| | |
|--|--------------------------|
| B Completed their mandatory training in the last 12 months | <input type="checkbox"/> |
|--|--------------------------|

2. The people involved in handling the information assets discussed in this document have the following training needs:

3. The following people have been involved in drafting, reviewing and submitting for approval this Privacy Impact Assessment (select all that apply):

| | |
|------------------|--------------------------|
| A Senior Manager | <input type="checkbox"/> |
|------------------|--------------------------|

| | |
|--------------------------|--------------------------|
| B The Caldicott Guardian | <input type="checkbox"/> |
|--------------------------|--------------------------|

| | |
|--|--------------------------|
| C The Senior Information Risk Officer (SIRO) | <input type="checkbox"/> |
|--|--------------------------|

| | |
|-----------------------------------|--------------------------|
| D The Information Governance Lead | <input type="checkbox"/> |
|-----------------------------------|--------------------------|

| | |
|----------------------------|--------------------------|
| E Providers of IT services | <input type="checkbox"/> |
|----------------------------|--------------------------|

| | |
|----------|--------------------------|
| F Others | <input type="checkbox"/> |
|----------|--------------------------|

4.

Please attach to this document any records of these discussions e.g. emails or minutes of meetings

5. Comments from Information Governance

6. Please record details of the sign off of the PIA

Name and signature of the person who/ chair of the group that approved the PIA

Role of the person who approved the PIA

Date approved

Date PIA to be reviewed

7. **For the approving person/group:** do you have any comments on this PIA?



End of Section E

Section E: Risk Assessment Guidance

Risks to Individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate Risks

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Non-Compliance Risks

- Non-compliance with the DPA.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Approaches to mitigating risks

Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

APPENDIX D - EQUALITY IMPACT SCREENING MATRIX

This equality impact screening matrix is intended to identify if the implementation of a new system being introduced by BrisDoc might adversely affect someone with a protected characteristic and/or risk BrisDoc breaching its Public Sector Equality Duty or fail to comply with the Equality Delivery System. Key criteria will be considered against each protected characteristic and if the implementation of the policy, project etc. would cause, or would have the potential to cause, an adverse impact on the person a full equality impact assessment should be undertaken.

| | | Yes / No | Comments |
|---|--|----------|----------|
| 1 | Does the policy/guidance affect one group less or more favorably than another on the basis of: | | |
| | Age | | |
| | Disability | | |
| | Religion or belief | | |
| | Sex | | |
| | Sexual Orientation | | |
| | Marriage/Civil Partnership | | |
| | Pregnancy and maternity | | |
| | Gender reassignment | | |
| | Race | | |
| 2 | Is there any evidence that some groups are affected differently? | | |
| 3 | If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable? | | |
| 4 | Is the impact of the policy/guidance likely to be negative? | | |
| 5 | If so can the impact be avoided? | | |
| 6 | What alternatives are there to achieving the policy/guidance without the impact? | | |
| 7 | Can we reduce the impact by taking different action? | | |

If you have identified a potential discriminatory impact of this document, please progress to undertaking a full equality impact assessment.