Information Governance Staff Handbook 2021-2022

Created: March 2021

Controlled by: Deb Lowndes

Job Title: Programme and Service Director

Version: 4.0

Review: March 2022

Reviewed on: March 2021

Reviewed by
Name: Sarah Pearce
Job Title: Compliance Officer

Signed by Director
Name: Nigel Gazzard

Signature:
Job Title: Managing Director

Document control

Date	Version	Author	Comments
March 2021	1.0	DL	First Draft
May 2021	2.0	DL	Comments from NC and SP
July 2021	3.0	DL	Final version for issue
August 2021	4.0	DL	KR Review

Table of Contents

Introduction

BrisDoc provides patients with a CONFIDENTIAL service.

This can only be achieved if **all staff** working for the service truly **understand** the term confidential and how to ensure that confidentiality is protected, whilst also recognising the need for appropriate information sharing to aid good care.

Good information Governance (IG) underpins good care, patients must feel assured that their information is used appropriately. You can help with this by following the good practice set out in this handbook.

Information Governance is the practice by which organisations ensure information is efficiently managed and that appropriate policies, system processes, effective management and accountability are in place to safeguard information.

Information Governance helps organisations to embed policies and processes to ensure that personal data is:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, and not excessive
- Accurate and kept up to date
- Kept for no longer that is necessary and
- Processed in a secure manner.

Information Governance also applies to corporate information and commercially sensitive data.

Information Governance is the responsibility of **EVERYONE** in BrisDoc.

BrisDoc holds large amounts of personal, commercially confidential, and special categories of personal data, and all staff should ensure that Information Governance standards are incorporated in their working practices.

BrisDoc must be able to evidence its compliance with data protection legislation.

Part 1 of this handbook provides a summary of the legislation and regulations that all staff should be aware of. Part 2 provides practical advice and information about key activities which will help to ensure compliance.

Part 1: Background & Legislation

1. Legislation and regulations

Staff should know their responsibilities under the data protection legislation that governs how organisations use and safeguard data and information, how individuals can exercise their rights under that legislation.

This area is complex but can be viewed as follows.

Data protection legislation is used as a generic term which encompasses the following:

- Data Protection Act 2018 (DPA 2018)
- Records Management Code of Practice for Health and Social Care 2016

In addition, BrisDoc must take account of the following legislation:

- Freedom of Information Act 2000
- Environmental Information Regulations
- INSPIRE Regulations
- Health and Social Care Act 2012
- Access to Health Records Act 1990
- Public Records Act 1958
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988.

BrisDoc has a suite of Information Governance policies, processes, and procedures, which can be found on Radar (BrisDoc's Intranet) or on local Service shared drives. There are additional Standard Operating Procedures (SoPs), which will detail the practical implementation of these policies. All staff should understand and comply with these SOPs. If in doubt ask your line manager.

Adherence to the principles of Information Governance supports compliance with the law and best practice. It also embeds processes that help staff manage data and information appropriately.

It must also be noted that embedding Information Governance processes gives patients, service users and the general public greater trust in BrisDoc Services and enables effective working across partner organisations.

2. Roles within the organisation

To support the assurance responsibility for information within BrisDoc, there are several key roles

- The Senior Information Risk Officer - Nigel Gazzard
- Caldicott Guardian - Dr Kathy Ryan
- Data Protection Officer – Affinity Resolutions (external)
- Information Security Manager - Debs Lowndes

They are supported by Heads of Service and Corporate Leads e.g., Practice Managers, Head of Workforce and Head of Integrated Urgent Care.

This group of staff make up the Information Governance Board, that meets quarterly.

All Staff

All staff have a legal duty of keep confidential data private and secure and not to divulge information, accidentally, or initentailly.

Staff may be held personally liable for a breach of confidence and must not:

- Talk about confidential matters in public places or where they can be overheard
- Leave any assets containing personal, commercially confidential, or special categories of personal data lying around unattended - this includes telephone messages, computer printouts, faxes and other documents
- Leave a computer logged on to a system where information can be accessed or viewed by another person without authority to view that information
- View any healthcare record without a legitimate reason i.e., specifically in relation to their role. Unauthorised access to health records will be viewed as a serious breach of confidentiality and will invoke action under BrisDoc's Disciplinary policy, which may result in dismissal

Staff must not use someone else's password to gain access to data. Action of this kind will be viewed as a serious breach of confidentiality under the Computer Misuse Act 1990 and in breach of Service IT policies. This is a disciplinary offence and could constitute gross misconduct which may result in dismissal.

3. Caldicott principles and Data Protection Legislation principles

The National Data Guardian (Dame Fiona Caldicott) made recommendations to improve the way the NHS uses and protects confidential information in the form of the Caldicott Principles; these have been updated in subsequent reviews.

The seven Caldicott principles support the confidentiality and security controls on using patient information. The principles should be used whenever a use of confidential information is being considered and in particular when there is an intention to transfer confidential information to another organisation

Principle 1: Justify the purpose - Why is the information needed?

Principle 2: Don't use personal confidential data unless absolutely necessary – Can the task be carried out without identifiable information?

Principle 3: Use the minimum necessary personal confidential data – Can the task be carried out with less information?

Principle 4: Access to personal confidential data should be restricted to required/relevant personnel.

Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities – Lack of knowledge is not acceptable

Principle 6: Understand and comply with the law.

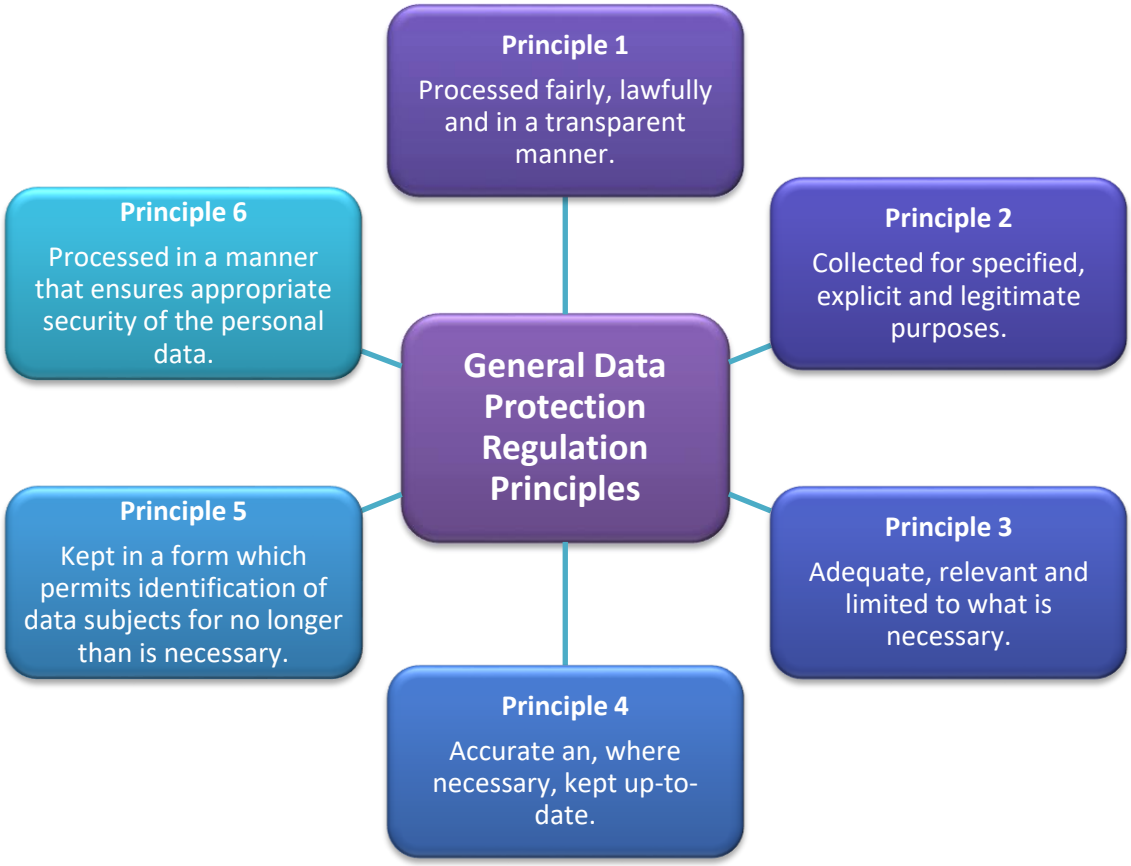
Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality

All organisations in the UK must comply with the data protection legislation which is defined in the Data Protection Act 2018 part 1(3)(9). The data protection legislation is enforced in the UK by the Information Commissioner's Office (ICO) who has the power to impose penalty notices on organisations based on two tiers - the "higher maximum amount" up to €20m or 4% of total annual turnover, whichever is the greatest; or the "standard maximum amount" up to €10m or 2% of total annual turnover, whichever is the greatest.

Accountability: GDPR Article 5 (2) "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

BrisDoc is the data controller (when we are the originator of the data e.g EMIS or Adastra patient record, data processing when we are using other systems e.g Connecting Care) and under the legislation it is not just data breaches which can attract a fine, non-compliance with the regulations can also be subject to fines which is why under the additional new data protection concept of 'accountability' organisations must be able to provide evidence of compliance.

A further set of six General Data Protection Regulation principles (Article 5) that must also be followed when handling personal and special categories of personal data. These regulations should be considered when handling both corporate and clinical records.



In addition, the Data Protection Legislation requires the 'controller' (see definitions above) to demonstrate compliance with these principles.

Data protection legislation and the Caldicott principles translate into **key rules for all staff to follow:**

- Patients and staff should be fully informed about how their information may be used.
- There are strict conditions under which personal and special categories of personal data may be disclose
- Individuals have rights including the right to information, the right of access, the right to rectification and erasure, the right to restrict processing, the right to data portability and the right to object to various types of processing of their data
- Identifiable information should be anonymised or pseudonymised wherever possible
- The disclosure or sharing of personal data is permissible where there is a legal obligation to do so, or an exemption can be applied or where the individual has given explicit consent
- Sharing of personal data between organisations can only take place with appropriate authority, safeguards, and agreements in place
- Sometimes a judgement has to be made about the balance between the duty of confidence and disclosure in the public interest. Any such disclosure must be justified
- Personal data should be always kept secure and confidential
- An organisation must be able to provide evidence to show compliance with the data protection legislation

Part 2: Practical Advice

Below you will find some practical advice that applies to your role to your role

2.1 Data Security

- Follow organisation policies
- Protect information physically
- Practice safe password management
- Transfer information securely
- Report breaches of security to management via the incident portal link on the BrisDoc website via the incident portal found on the weblinks page

Passwords – Create strong memorable passwords, such as by using three random words. Avoid using predictable passwords, such as dates, family, and pet names. Some systems will require a mix of letters, numbers, and special characters.

Away from your desk – always lock your PC when away from your desk

Eavesdropping - Be careful that your conversations are not overheard by people who do not need to know.

Physical Security - Keep doors closed to restricted areas and be aware of strangers entering buildings, challenge them if not wearing a visitors badge.

Email - Ensure you know **who** you are sending information to before you press 'send'.
Check the address if you are unsure. Only ever send confidential or sensitive data to a trusted NHS.NET or NHS.UK address.

Think Before You Click - The most common way ransomware enter networks and computers is through email. Often, scammers will include malicious links or attachments in emails that look harmless.

To avoid this trap, please observe the following email best practices:

- Do not click on links or attachments from senders that you do not recognise
- Be especially wary of .zip or other compressed or executable file types
- Do not provide sensitive personal information (like usernames and passwords) over email
- Watch for email senders that use suspicious or misleading domain names
- If you can't tell if an email is legitimate or not, please delete it and raise a digital support ticket

If something seems wrong, DELETE IT. If it's legitimate, they will email again.

Internal & External Mail - Ensure you are using the most up to date and confirmed address details and use the full address.

Fax - Confirm the fax number and that someone is there to receive the fax before pressing 'send'. Only to be used where operationally required e.g. as a business continuity solution.

Smartcard – always keep your card and password safe. If you loose your card inform your line manager immediately.

Telephone Security - Confirm the identity of the caller and justify the need to disclose confidential information to them before doing so. If in doubt, ask for something in writing or that you will call them back.

Training - Make sure that you and your colleagues are aware of information governance and complete relevant IG training annually.

If In doubt, call it out - Reporting incidents promptly via the Digital Team/IT Leads or your line manager – can massively reduce the potential harm caused by cyber incidents.

Security incidents include:

- **Information disclosed in error** – Think about faxes sent to the wrong number
- **Lost data/hardware** – Think about an unprotected memory stick left in a public area
- **Breach arising from non-secure disposal** – Think about putting paper notes in a domestic rubbish bin
- **Information lost in transit -** Think about prescriptions sent in the post
- **Stolen data or hardware** – Think about the risk of laptops being stolen from vehicles etc
- **A technical or procedural failure** – Think about paper processes when systems like EMIS and Adastra fail

Incident forms are quick to complete, incident forms are available on the Radar home page and Clinical Toolkit

See below for examples of Risks to be aware of

Scenario - Last week, someone in a high visibility vest visited a Social Care office as well as a GP practice. He followed a member of staff into the building and told the receptionist that he needed everyone's details for a 'software update'. He then sold these details to other criminals. Let's find out what else he found……

- **Doors**: Nearly every door was open; even "restricted access" doors had been propped open to allow for a delivery.
- **Visitors**: The receptionist was happy to direct him to the server room…he wasn't even asked to sign in or show a visitor's badge.
- **Desks**: There was so much information in unoccupied office areas. He randomly dispersed memory sticks on the desks; hopefully someone will plug one into their machine and it can start installing malware.

- **Other areas**: The server room door was unlocked, meaning he could disrupt the server causing connectivity problems. As there is so little physical security, he can potentially come and go as he pleases…perhaps next week.

2.3 Business Continuity

- Business Continuity is the plan that BrisDoc must execute to ensure we are able to provide services to patients, regardless of what might happen to resources, infrastructure, or facilities.
- Action plans identify the risk of events and how they will be responded to, in the event of a loss of service e.g., Gas, IT systems, Buildings Services. Action plans are managed and held by Service Managers and Duty Managers. Copies are on radar and held at bases.
- To help, make sure you know where the Business Continuity box is in your base and the processes within it.

2.4 Practical notes for your role in BrisDoc

General Practice and Homeless Health Service Staff

- If speaking to patients directly, speak quietly but clearly, respect their privacy. Let them confirm their details to you
- Keep a neat and tidy desk and as paper free as possible
- Keep passwords strong and secure, don't use your D.O.B or pet names. Your password should not be guessable! Don't share passwords
- Report information security related incidents via the incident reporting portal on radar or the BrisDoc website
- If you are unsure of an information related issue speak to the Practice Manager, or most senior Manager working with you
- Be aware of the location of the Business Continuity box and processes within it
- Be vigilant when at a base, consider what information you have access to and guide staff, where observations are made that might cause an issue
- Always perform a 'local' search before entering new patients to avoid duplication. (the local search reviews patients who have attended the practice, WIC or HHS before). Always search SCR (summary care record) to perform a wider, national search of the NHS Spine for patients who haven't visited before but who have an existing NHS number. Confirm details with the patient. Only use free text demographic information if the patient hasn't been registered with a GP in England before. Sometimes the patient is registered on the 'NHS spine' with an old address or contact telephone number. Confirm with the patient that this is their previous information and update EMIS. Patients whose information does not match the spine are indicated on EMIS with the PDS (Patient demographic service) symbol on the demographic bar being 'RED' rather than 'BLUE'. If this box is clicked on, you can choose the correct information and update the 'spine'. Updating the spine is helpful as it ensures that duplicate records aren't created for patients and all patient's medical information is kept up to date and accurate
- When faxing, ensure use of a fax header and shred paperwork once confirmation is received
- When sending paperwork, always ensure the address on the envelopes is correct. Mark the envelope as private and confidential and use a return to sender sticker on the reverse

General Practice and Homeless Health Service Staff Clinical Staff

- Report information security related incidents to the Practice Manager
- Always code against the appropriate heading. 'e.g., problems against problems and procedures against procedures etc
- If you are unsure, do not code. Make enquiries or find suitable evidence before proceeding
- Only code events that are evidence based. Do not code based on assumptions
- When speaking to colleagues always be discreet, discuss in private and not in front of other patients / people. Patients should only be discussed in front of people who are or may become involved in their care

IUC Hosts

- Ensure all data collected is inputted and confirmed correctly onto Adastra i.e. spelling of names. correct D.O.B, address, and surgeries
- Let the patient or professional confirm details to you, ask them to re-confirm the information you may already have as not doing so this may lead to old information being held
- When faxing prescriptions, always use a fax header, and ensure the fax number is correct
- When sending paperwork always ensure always ensure the address on the envelopes are correct. Mark the envelope as private and confidential and use a return to sender sticker on the reverse
- Do not include any personal or confidential data on fax headers
- If case notes are to be faxed, ensure use of a fax header and shred case notes once fax sent confirmation is received
- Do not leave any unnecessary paperwork lying around once dealt with
- Always when speaking to colleagues about a patient, be discreet and discuss in private and not in front of others
- If speaking to patients directly on arrival to base speak quietly but clearly, respect their privacy. Let them confirm their details to you
- Keep a neat and tidy desk and as paper free as possible
- If you are unsure of an information related issue, please ask the shift manager
- Keep passwords strong and secure, don't use your D.O.B or pet names. Your password should not be guessable! Don't share passwords
- Report information security related incidents to your Shift Manager
- Be aware of the location of the Business Continuity box and processes within it

IUC Drivers

- Keep the car clear of any unnecessary paperwork i.e., case notes and shred all notes on completion of your shift
- File all Driver log sheets appropriately at end of shift
- Always keep track of tough books as they hold vital personal information
- Keep passwords strong and secure, don't use your D.O.B or pet names. Your password should not be guessable! Don't share passwords
- If discussing a patient, be discreet. Stay in the car and not on the street or in front of other people
- Be aware of the location of the Business Continuity box and processes within it
- Report information security related incidents to your Shift Manager via the incident reporting portal on radar or the BrisDoc website

IUC WACCS

- Ensure all data collected is input and confirmed correctly onto Adastra i.e. spelling of names. correct D.O.B, address, and surgeries
- Let the patient or professional confirm details to you, ask them to re-confirm the information you may already have as not doing so may lead to old information being held.
- Do not leave any unnecessary paperwork lying around once dealt with. All Despatch sheets to be filed away
- Shred all case notes and paperwork if not required
- If paperwork is to be faxed or e-mailed, double check you have the correct address or number to ensure personal information is sent to the correct place
- Always when speaking to colleagues about a patient, be discreet and discuss in private and not in front of others
- If speaking to patient directly speak quietly but clearly, respect their privacy. Again, let them confirm their details to you
- Keep a neat and tidy desk and as paper free as possible
- Keep passwords strong and secure, don't use your D.O.B or pet names. Your password should not be guessable! Don't share passwords
- Report information security related incidents to your Shift Manager via the incident reporting portal on radar or the BrisDoc website
- Be aware of the location of the Business Continuity box and processes within it

IUC Shift Managers and Team Leaders

- Ensure all data collected is inputted and confirmed correctly onto Adastra i.e. spelling of names. correct D.O.B, address, and surgeries
- Let the patient or professional confirm details to you, ask them to re-confirm the information you may already have as not doing so may lead to old information being held.
- Do not leave any unnecessary paperwork lying around once dealt with
- If paperwork is to be faxed or e-mailed, double check you have the correct address or number to ensure personal information if sent to the correct place
- Always when speaking to colleagues about a patient, be discreet and discuss in private and not in front of other patients
- If speaking to patients directly, speak quietly but clearly, respect their privacy. Let them confirm their details to you
- Keep a neat and tidy desk and as paper free as possible
- Keep passwords strong and secure, don't use your D.O.B or pet names. Your password should not be guessable! Don't share passwords
- Report information security related incidents to BrisDoc's Head of Governances via the incident reporting portal on radar or the BrisDoc website
- Be aware of the location of the Business Continuity box and processes within it
- Be vigilant when at a base, consider what information you have access to and guide staff, where observations are made that might cause an issue

Call Handlers

- Ensure all data collected is inputted and confirmed correctly onto Adastra i.e. spelling of names. correct D.O.B, address, and surgeries
- Let the patient or professional confirm details to you, ask them to re-confirm the information you may already have as not doing so this may lead to old information being held
- When faxing prescriptions, always use a fax header, and ensure the fax number is correct

- Do not include any personal or confidential data on fax headers
- If case notes are to be faxed, ensure use of a fax header and shred case notes once fax sent confirmation is received
- When sending paperwork, always ensue the address on the envelopes are correct; Mark the envelope as private and confidential and use a return to sender sticker on the reverse
- Do not leave any unnecessary paperwork lying around once dealt with
- Keep a neat and tidy desk and as paper free as possible
- If you are unsure of an information related issue, please ask the Service Manager
- Keep passwords strong and secure, don't use your D.O.B or pet names. Your password should not be guessable! Don't share passwords
- Report information security related incidents to the Service Manager via the incident reporting portal on radar or the BrisDoc website
- Be aware of the location of the Business Continuity Folder and processes within it
- Shred all case notes and paperwork if not required
- Ensure accurate record keeping at all times

IUC Clinicians

- Ensure yourpatient case notes are inputted correctly onto Adastra
- Adhere to local processes around the management of prescriptions, ensuring they are given directly to patients and not left on desks or clinical areas
- Do not include any personal or confidential data on fax headers
- If case notes are to be faxed, ensure use of a fax header and shred case notes once fax sent confirmation is received
- Do not leave any unnecessary paperwork lying around once dealt with
- Ensure accurate record keeping at all times
- Always when speaking to colleagues about a patient, be discreet and discuss in private and not in front of others
- Keep a neat and tidy desk and as paper free as possible
- If you are unsure of an information related issue, please ask the Service Manager
- Keep passwords strong and secure, don't use your D.O.B or pet names. Your password should not be guessable! Don't share passwords
- Report information security related incidents to the Service Manager. via the incident reporting portal on radar or the BrisDoc website
- Be aware of the location of the Business Continuity Folder and processes within it
- Shred all case notes and paperwork if not required
- When seeing patients, ensure that conversations about their condition or treatment are held privately

Managers and Corporate Admin Staff

- Ensure all data collected is input and confirmed correctly onto IT Systems e.g. spelling of names, correct D.O.B, address, surgeries, staff details and incident summaries
- Let the patient, professional or staff member confirm details to you, ask them to re-confirm the information you may already have as not doing so may lead to old information being held
- Do not leave any unnecessary paperwork lying around once dealt with
- If paperwork is to be faxed or e-mailed, double check you have the correct address or number to ensure personal information is sent to the correct place
- Always when speaking to colleagues about a patient or staff member, be discreet and discuss in private and not in front of other people

- If speaking to patients directly, speak quietly but clearly, respect their privacy. Again, let them confirm their details to you
- Keep a neat and tidy desk and as paper free as possible
- Keep passwords strong and secure, don't use your D.O.B or pet names. Your password should not be guessable! Don't share passwords
- Report information security related incidents to BrisDoc's Head of Governance. via the incident reporting portal on radar or the BrisDoc website
- Be aware of the location of the Business Continuity box and processes within it
- Be vigilant at your place of work, consider what information you have access to and where observations are made that might cause an issue, guide staff with respect to behaviour and appropriate actions to take

Summary

- If in doubt ask
- Keep your understanding of SoPs that apply up to date
- Keep your training up to date