Information Governance Framework

Policy data sheet

Policy Name:	Information Governance Framework
Document Reference:	BLG0052
Version Number:	10
Ratified By:	Executive Team
Exec Team Ratified Date:	May 2024
Review Period:	3 Years
Review Date:	May 2027

Contents:

ADVICE: Before using this document you should ensure that you have the most up-to-date version. If you are referring to a printed version it may be out-of-date. If in any doubt please check with Human Resources.

Information Governance Framework

1. Aim of the Framework

The aim of this framework is to recognise and manage the risks to information security and to ensure The Big Life group has quality data resources which are accurate and appropriately accessible. It provides high level guidance for ensuring the confidentiality, integrity and availability of information and is supported by detailed group policies and business-level operational procedures.

Confidentiality – data access is confined to those with specified authority to view the data.
Integrity – all information systems are operating according to specifications which ensure information is secure, accurate and appropriately accessible.
Availability – information is delivered to the right person when it is needed.

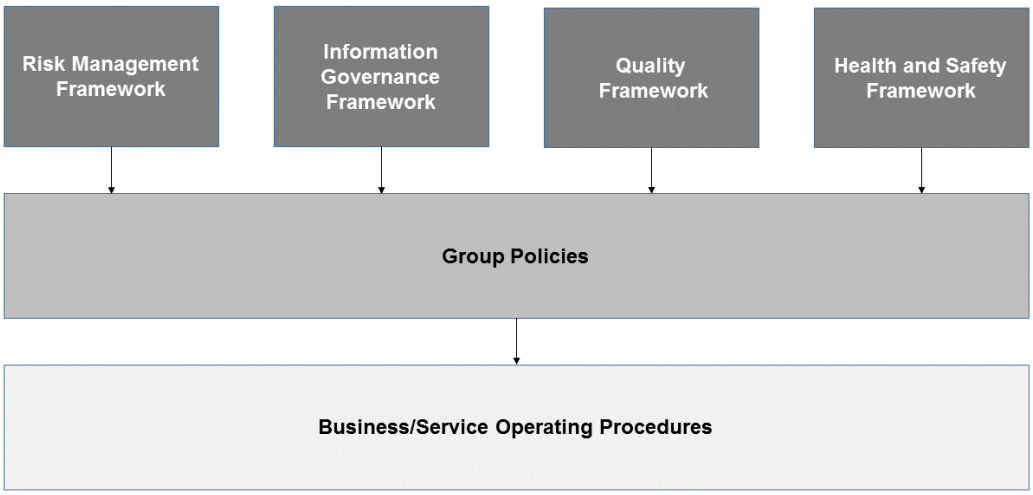
Whilst information governance in particular outlines the way that personal or sensitive client information should be protected and ensures compliance with statutory requirements, it also underpins clinical, service and corporate governance. Statutory legislation includes:

- The Data Protection Act 2018
- Access to Health Records Act 1990
- The Human Rights Act 1998
- Crime and Disorder Act 1998
- Health and Safety at Work Act 1974
- Freedom of Information Act 2000.
- General Data Protection Regulations

The Framework puts into practice the Caldicott Principles, which have been developed to protect the confidentiality of patient information. They are applicable to all identifiable patient or service user information:

- Justify the purpose(s) for using/sharing confidential information
- Only use confidential information when absolutely necessary
- Use only the minimum confidential information that is required
- Access to confidential information should be on a strict need to know basis
- Everyone with access to confidential information should be aware of and understand their responsibilities
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality

This framework is one of 4 frameworks within the group, which sit above the group policies and business/service operational procedures as per the diagram below.



2. Scope

This framework outlines all the systems, processes, roles and accountabilities for ensuring that information is secure, appropriately accessible and accurate. Where systems or information are managed by third parties, they are required to operate in line with this framework. The framework covers both manual and electronic data. The chart below describes all the areas contributing to this framework. Shaded areas are detailed within this framework. Unshaded areas are detailed in other associated policies and documents, which can be found on the Hub

Governance	Workforce	Environment	Clinical and Service Care	Learning
Board and Trustees	Policies and Procedures Refer to associated policies as listed in this framework	Record Keeping and Data Protection Policy	Information Sharing	Incident and serious and untoward reporting policy
Risk and Quality Committee	Staff training	Information Asset Register and	Client consent and access to records	NHS duty of: Being Open

ADVICE: Before using this document you should ensure that you have the most up-to-date version. If you are referring to a printed version it may be out-of-date. If in any doubt please check with Human Resources.

		Retention Schedule		and Duty of Candour
Information Governance Framework	ISO 9001 and BS7799	Software protection	Data quality control and data validation	
Audit	User Access Control	Equipment control	Online and social media Policy	
		Business Continuity Plans	Safeguarding Children , young people and Vulnerable Adults	
		Decommissioning and recycling IT equipment		
		IT internet and email policy		
		Information Security		

3. Roles and Responsibilities

Board
The ultimate responsibility for information governance rests with the Board of Directors, who ensures there are adequate controls within the group; appoints a Caldecott Guardian; and receives assurance reports from the Quality Committee

Quality Committee. Attended by the Information Governance Lead (DPO) and Caldicott Guardian. Reviews staff training receives a report on an assessment of information governance, and reviews all serious incidents involving actual or potential loss of data or breach of confidentiality.

Executive Team
Responsible for the day-to-day operation of the group and ensuring that staff, systems and sub contractors comply with the requirements of the Information Governance Framework and associated policies. Responsible for appointing the Data Processing Officer/Information Governance Lead.

Data Protection Officer/Information Governance Lead
Provides assistance to monitor internal compliance, informs and advises on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. Ensures the Framework and Policies are updated in line with best practice and learning; and participates in the investigation and reporting of information incidents.

Caldicott Guardian
The Caldicott Principles have been developed to protect the confidentiality of client information. They are applicable to all identifiable and sensitive client information. The Principles are:

- Justify the purpose(s) for using confidential client information
- Only use confidential information when absolutely necessary
- Only use the minimum confidential information that is required
- Access should be restricted on a need-to-know basis
- Everyone should be aware of and understand their responsibilities
- Use and handling of personal identifiable information should comply with the law. (refer to **Keeping Records and Data Protection** Policy)
- The duty to share information can be as important as the duty to protect patient confidentiality

The Caldicott Guardian within The Big Life Group is responsible for protecting the confidentiality of personal information and enabling appropriate information sharing, the guardian is a member of the Board, Risk and Quality Committeeand the Executive Team.

Managers
Managers are responsible for ensuring that their staff understand and comply with their data access levels and Information Governance policies and procedures. They ensure through completing the new starter and leaver processes that the asset register has an up to date record of which staff are allocated equipment. They approve staff access levels and ensure the compliance of all policies and procedures within the framework.

Staff
All staff members are required to comply with this framework, associated policies and business-level operational procedures in their day-to-day work and to report any incidents as outlined in the policies and procedures.

Sub-contractors and third parties
Are required to comply with this framework, associated policies and business-level operational procedures and to report any incidents as required. This forms part of the initial due diligence and service level agreement. All ICT suppliers need to undertake an Information Security due diligence check by the Head of Applications and Development or Head of IT during the procurement process.

4. Equipment Control

The effective management of information assets (e.g. laptops, mobiles, software licences) is essential for effective information governance. The management of information assets is necessary for the following

- Ensuring all equipment is insured
- Preventing equipment from being lost or stolen
- Ensuring equipment has appropriate virus protection

- Ensuring software licences are up to date
- Ensuring that there is secure disposal of equipment when it is no longer usable

The effective use of asset registers facilitates the management of information assets. The Head of IT is responsible for developing and reviewing policies and procedures for using asset registers. All staff members are required to adhere to these policies and procedures.

5. Information Security

A central tenet of Information Governance is to safeguard information from loss, destruction, theft or unauthorised disclosure; this information may be held on computerised information systems, manual files, reports and other written communications. Data Protection legislation requires organisations to implement proportionate controls to safeguard information. Information Security is covered in detail in the Information Security Policy; only a brief high level summary is presented here.

Data Classification

The Big Life group classifies its data, based on its sensitivity, value and criticality to ensure that all sensitive data is secured and shared appropriately. The **Data Classification Policy** sets out the group's approach to this.

Storage

All group electronic information must be stored in a secure environment with robust controls to protect against physical and network risks. These controls must include effective data backup, firewalls, physical protection, and user access regimes. No information should be stored outside the EU without specific assurances that storage adheres to legal, regulatory and contractual requirements. Where an IT contractor is used, the service level agreement must include clauses which provide assurance as to their information security procedures and compliance with the group's legal, regulatory, and contractual requirements.

Manual files containing personal identifiable information must be kept in locked and secure storage and must be reviewed in line with the group's retention schedule.

Confidential information should not be left on desks unattended and electronic records should not be left open on computers unattended.

Paper records should not be removed from the premises unless authorised, absolutely necessary and a risk assessment has been undertaken. They should not be taken to staff homes or kept in cars.

Access

Remote access to electronic information is controlled by the use of secure login by authorised staff members and role-based access. Personalised access credentials

(i.e. password,) must be used only by the individual that they pertain to. The use of shared access credentials should be minimised and tightly controlled.

Accessing information must be in accordance with Caldicott principles. Where possible, information should only be accessible to those staff members who need to access it for the purpose of undertaking their role. However, access requirements may be complex and dynamic and the use of technological controls to restrict access can lead to other risks.

Therefore, all staff members/volunteers have a responsibility only to access and process information for the purpose of performing work related duties.

Transfer

On occasions it may be necessary to transfer personal identifiable or sensitive information and this may lead to risks of loss or disclosure. To ensure that these risks are mitigated, relevant staff and managers must adhere to the relevant sections of the Information Security Policy. Where the transfer is not covered by established group procedures, the IG Lead or must be consulted prior to transfer to ensure risks are assessed.

Deletion/Disposal

If it is appropriate to delete or dispose of information, this needs to be undertaken securely. Paper that contains confidential information must be shredded using a crosscut shredder, or alternatively secure waste collection by an approved provider can be used. Electronic information should be securely deleted. Deletion of data should align to the group **Data Retention Schedule.**

Availability

To ensure that information is delivered to the right person when it is needed, data is backed up, following a 3-2-1 approach and in line with the Group's **Back-Up Policy**.

Risk Management

Wherever sensitive information is processed (i.e. stored, transfer, disposed), risk assessments must be undertaken regularly to ensure all controls are as effective at mitigating risk. In information risk management, risk assessments are called Data Protection Impact Assessments (DPIA). You must liaise with the Data Protection Officer/Information Governance Lead for advice on whether a full DPIA is needed. DPIAs must

- describe the processing and your purposes;
- assess necessity and proportionality;
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data

DPIAs must be undertaken with the support of the Data Protection Officer/Information Governance Lead, and using the template document (BLG244) which has been developed based on the ICO's template and guidance for DPIAs

https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf If you are required to follow a different template please liaise with the Data Protection Officer.

Where significant risks are identified, for which there is no immediate mitigation, an action plan must be developed. The Information Governance Lead and Caldicott Guardian must also be informed, and the business must include the risk on their risk register (see Risk Management Framework) until it is satisfactorily mitigated

When a new process or project is implemented – the risks to data protection can be increased, and Information risks must be properly accounted. There must be consideration of whether a DPIA needs to be included as part of the overall risk assessment for the project. The group maintains a record of data processing activities – this needs to be amended when new processes are implemented.

6. Internet, Email and Social Media

The internet, email and social media are essential tools within the work environment. However, there are also significance information governance risks associated with using such applications. Guidelines for the appropriate use of Internet, email and social media are contained within the**ICT Acceptable Use policy**. All staff members must ensure that they understand and work within the guidelines of this policy.

7. Record Keeping and Data Quality

The group is required to keep appropriate and accurate records. Recorded information must contain no more personal/sensitive details than are necessary, be accessible, and be accurate. Inaccuracies have the potential to adversely affect Information Governance, client care and business performance. Information recording is the direct responsibility of the person inputting the data, supported by their line manager. Wherever possible, systems should be adopted that identify and flag potential data errors. Managers should ensure that they operate systems to validate and audit information and data systems at regular intervals.

Managers are responsible for ensuring that information is kept no longer than is necessary according to legislative and regulatory requirements that apply to the information being stored. Details regarding retention can be found in the retention schedule for the service (BLG257). Information that does not need to be retained must be securely disposed of. Paper records and information that need to be retained but is not required for day-to-day operations can be stored at the group archive. If you are required to archive any information, please contact the Quality Team (training@thebiglifegroup.com) for guidance on how to do this.

Detailed guidance for keeping records and data quality can be found in the group's **Keeping Records and Data Protection** Policy and business-level operational procedures.

8. Access Rights

Legislation exists which stipulate rights for individuals, their representatives, or external agencies to gain access to information that organisations hold.

Specifically, the Data Protection Act/GDPR provides for subject access rights where individuals have the right to access information that an organisation holds about them. In some circumstances the Freedom of Information (FOI) Act applies. This Act provides a public right of access to information held by public authorities. The Big Life group is not a public authority. However, since some of the group's contracts are delivered for public authorities, some information the group holds would require disclosure under the FOI Act.

The Big Life Group must ensure that arrangements are in place to facilitate access rights stipulated by legislation. Detailed guidance can be found in **Keeping Records and Data Protection policy** and business-level operational procedures.

9. Information Sharing

Information that the group collects pertaining to individuals is 'confidential'. The consequence of this designation is that there are rules or controls for how this information is shared. Detailed guidance is found in the **Confidentiality Policy**, which outlines the situations for which information can be shared with or without an individual's consent.

Where services operate in partnership with other organisations delivering integrated services it is often routinely necessary to share information. Depending on the volume of information sharing, an Information Sharing Agreement (ISA) should be considered. An ISA in itself does not permit information sharing nor negate our responsibilities under data protection legislation; however, the development of an ISA will help ensure that information sharing is legal.

10. Staff Training

All staff members must undertake Information Governance Training. The level and format of the mandated training is dependent on a staff member's role. Mandatory training requirements are determined by the Information Governance Lead/Data Protection Officer and Business Leads on an annual basis and incorporated into the training plans. Staff can see the training they are required to complete on the group's online training platform (Learn Well) and when a renewal is next due.

11. Business Continuity

All business areas within the group must include contingencies for information loss (temporary or permanent) within their Business Continuity Plan. All IT subcontractors must provide details as to their Business Continuity arrangements to the appropriate business lead within the group.

A separate IT Business Continuity Plan is maintained by the Head of IT and as part of an information security audit, all IT subcontractors must provide satisfactory details as to their Business Continuity arrangements

.

12. Incident

In line with the **Serious Untoward Incident and Incident policy**, any loss or breach of confidentiality, integrity or interruption to availability of data or information, must be treated as an incident and reported to the Information Governance Lead and included in reports to the Quality Committee. If the breach involves ICT, the group Head of IT should be informed as soon as possible to facilitate effective breach response. If the breach is serious, it must be investigated as a SIRI, with lessons learned, recommendations and an action plan. Consideration will be given by the Information Governance Lead and the Caldecott Guardian as to whether to inform those affected by the Information Breach. Where any risk of harm to clients is identified, those affected must always be informed. This approach is in accordance with the company's values and the 10 key principles underpinning the NHS requirements of Being Open and Duty of Candour

- Acknowledgement
- Truthfulness, timeliness and clarity of communication
- Apology if appropriate
- Recognising service user and carer expectations
- Professional support
- Risk management and systems improvement
- Multidisciplinary responsibility
- Clinical governance
- Confidentiality
- Continuity of care

Serious breaches must also be reported to Information Commissioners Office; the Caldecott Guardian must authorise all breach notification reports. Specific services may also need to report breaches to commissioners as determined by their contract.

13. Complaints

Complaints from clients must be dealt with according to the group's **Complaints Policy**; complaints from staff and volunteers must be dealt with according to the group's **Grievance Policy**. However the Information Governance Lead should be consulted for advice in all cases where a breach of information governance is alleged, as escalation to the Caldecott Guardian may be required for some complaints.

14. Reporting and Audits

Each business area will be audited at least annually by the DPO and quality team. Any areas for improvement should be recorded on the service's Continuous Improvement Plan and monitored through senior management team meetings.

The group DPO is responsible for submitting a quarterly and annual information governance report to the quality committee.

15. Freedom of Information

The Freedom of Information (FOI) Act provides public access to information held by public authorities.

It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland. Public authorities include government departments, local authorities, the NHS, state schools and police forces. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

The FOI act does not apply to the Big Life group directly. However, it does apply directly to some of the businesses in group (e.g. the schools), and indirectly to other businesses via work which is funded by public authorities.

In those cases where freedom of information applies directly, the business must have a procedure for responding to FOI requests from members of the public and complying to other terms of the Act. This procedure must be made publicly available.

In those case where freedom of information applies indirectly, all FOI requests or compliance issues must be directed to the responsible commission for their advice.

16.Associated policies

- Keeping Records and Data Protection
- Confidentiality
- Information Security
- IT, Email, social networking policy
- Serious Untoward Incident and Incident
- Safeguarding
- Data Retention Schedule
- ICT and Acceptable Use Policy
- Data Classification
- Back Up
- Retention