INFORMATION GOVERNANCE POLICY AND MANAGEMENT FRAMEWORK

BADGER GROUP
Badger House
121 Glover Street
Birmingham, B9 4EY

Destroy All Previous Issues

Contents

DOCUMENT CONTROL

Document Storage

P:\Ops Team\Central Policies & Procedures - Development - Word Docs\IG - IGSoc - GDPR Policies\IG-01 - Information Governance Policy V4.0.docx

Version Control Log

(Only last 3 versions, earlier versions can be found in the appropriate Archive directory for the document)

Version	Date	Author	Description of Changes
V3.0	April 2021	S Owen	Reviewed, minor changes
V3.1	April 2022	S Barnes	Under Review, minor changes to flow chart 5.4.1
V4.0	Sept 2023	J Carey	Reviewed, changes to sections 4-5 inc numbering and flowchart

Approval

Version	Name	Position	Signature	Approved Date
V2.0	IG Steering Group			14 March 2018
V2.1	Badger Executive	Executive Team		25 July 2019

Glossary

Term	Description
IGSG	Information Governance Steering Group
IG	Information Governance
SIRO	Senior Information Risk Owner
eLfH	eLearning for Health, an NHS Digital online training toolset
GDPR	General Data Protection Regulations
DSP	Data Security and Protection

1 INTRODUCTION

Information Governance is one of the main governance arrangements within Badger along with Clinical Governance, Risk Management and Financial Governance.
Information is a vital asset, in terms of the identification and screening of potential patients, clinical management of individual patients and the efficient management of services and resources. It plays a key part in the effective delivery of services, corporate governance, clinical governance, service planning and redesign, performance and business management and resource management.

It is therefore of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information governance. Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the business

This policy gives assurance to Badger's business partners and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible patient care. Badger will establish and maintain policies and procedures to ensure compliance with requirements contained in the General Data Protection Regulations (GDPR) and NHS Digital Data Security & Protection (DSP) Toolkit.

2 SCOPE

This policy applies to all employees (permanent, seconded, graduate management trainees, temporary staff and volunteers) and all independent contractors in Badger. All third party organisations with whom Badger may enter into information sharing agreements governed by the Badger information sharing protocols must be made aware of this policy.

This policy covers all aspects of information within the organisation, including but not limited to:

- Patient/ Client/ Service User Information
- Personnel information
- Organisational information
- Electronic records or patient only records
- Paper documentation

3 PURPOSE

Badger recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Badger fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard personal information about patients, staff and commercially sensitive information.

Badger recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and in some circumstances, the public interest. Badger believes that accurate, timely and relevant information is essential to deliver the highest quality health care.

This document the defines principles for Information Governance in compliance with national legislation and as recommended by NHS Digital, (see Appendix 1)

4 POLICY

The four key elements that make up the Information Governance Policy are:

- Openness

- Legal Compliance
- Information Security
- Quality Assurance

4.1 Openness

a) Non-confidential information about Badger and its services are made available to the public through a variety of media.

b) Badger will maintain policies to ensure consistency with the requirements of the GDPR. Patients should have ready access to information relating to their own healthcare, their options for treatment and their rights as patients.

c) Badger will have clear procedures and arrangements in place for handling queries from patients and the public.

d) Badger will have clear procedures and arrangements for liaison with the press and broadcasting media through the Chief Executive's Office.

4.2 Legal Compliance

a) In accordance with the Data Protection Act 2018, Badger regards all personal information as confidential information and will undertake/commission assessments/audits of its compliance with the relevant legal requirements

b) Badger has established and maintains procedures for the control and appropriate sharing of patient information with other agencies. These take into account relevant legislation (e.g. Health and Social Care (national Data Guardian) Act 2018, Crime and Disorder Act 1998, The Children Act 2004).

c) Badger will establish and maintain policies to ensure compliance with GDPR, the Data Protection Act 2018 (the Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'), Human Rights Act 1998 and the Common Law Duty of Confidentiality.

d) Badger regards all personally identifiable information and special category data relating to patients and staff as confidential and will not be disclosed without the appropriate consent. Exceptions to this exist where national policy on accountability and openness requires otherwise or where requested by appropriate legal authorities.

4.3 Information Security

a) Badger has policies for effective and secure management of its information assets and resources across the organisation and undertakes or commissions annual assessments and audits of IT security arrangements to ensure compliance with legal requirements.

b) Badger maintains incident reporting procedures and monitors and investigates all reported instances, or potential breaches, of information security and confidentiality.

c) Badger promotes effective information security and confidentiality through policies, procedures, and training opportunities.

d) Badger will ensure that additional security measures are in place to protect electronic health records, such as data encryption and access controls.

4.4 Information Quality Assurance

a) Badger will promote information quality and effective records management across the organisation via policies, procedures, guidelines/user manuals and training.

b) Data Standards will be set through clear and consistent definitions of data in adherence with national standards and professional code of conduct.

c) Information quality should be assured from the point of collection and throughout its lifecycle.

d) Badger will establish and maintain policies and procedures for information quality assurance and the effective management of records.

e) Badger will undertake or commission annual assessments and audits of its information quality and records management arrangements.

5 INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK

5.1 Senior Leadership Roles

This section outlines senior leadership roles, resources, and responsibilities, including Caldicott Guardian, Senior Information Risk Owner (SIRO), and Information Governance Lead.

Badger has developed several policies supporting the Information Governance Framework, including Governance Structure, Compliance, and Training, and Guidance.

Badger has established an IG Steering Group and ensures training and guidance are provided to staff, including new starters and annual training requirements.
The following table identifies the senior Information Governance roles within Badger. As an NHS Partner Organisation and a smaller organisation in Information Governance terms these roles are not undertaken as a full-time position.

For more information about the Caldicott Guardian refer to IG-03.

Primary Roles	Additional Roles in the Group	Name	Position in Badger
Caldicott Guardian	Clinical Requirements	Dr Vipran Vijaya	Group Medical Director
Senior Information Risk Owner (SIRO)	Policies	Dr Waqar Azmi	Chief Executive Officer (Board Member)
Information Governance Lead (IG Lead)	Policies, Audit, Assurance, Implementation	Jo Carey	Head of Performance and Quality

5.1.1 Caldicott Guardian

Responsible to: Badger Board

Job Summary:

The appointment of a Caldicott Guardian was one of the recommendations of the Caldicott Report published in December 1997. The role of the guardian is to safeguard and govern uses made of patient information within Badger, as well as data flows to other NHS and non-NHS organisations. Caldicott Guardianship is a key component of broader information governance.

The Guardian is responsible for the establishment of procedures governing access to, and the use of, person-identifiable patient information and, where appropriate, the transfer of that information to other bodies.

In addition to the principles developed in the Caldicott Report, the Guardian must also take account of the codes of conduct provided by professional bodies, and guidance on the Protection and Use of Patient Information and on IM&T security disseminated by the Department of Health, including the NHS Confidentiality Code of Practice.

Working Relationships

The Caldicott Guardian will be expected to liaise and work with Service Managers and the Badger Board in the course of promoting the Caldicott principles.

The Caldicott Guardian is a member of Badgers Information Governance Steering Group and will need to work closely with records management, HR, IM&T, and other colleagues from work areas represented on that group.

Through an established network of NHS and Social Services representatives, the Caldicott Guardian also contributes to the peer review and interpretation of local or national confidentiality issues and the development of standards throughout the local health and social care community and partner organisations.

The Caldicott Guardian is supported by the SIRO and the IG Lead.

Time Commitment

The amount of time spent on Caldicott work will vary from week to week depending on scheduling of meetings and ad hoc demands.

Key Tasks

Production of Procedures, Guidelines and Protocols

- To oversee development and implementation of procedures that ensure that all routine uses of person-identifiable patient information are identified, agreed as being justified and documented.
- To oversee development and implementation of criteria and a process for dealing with ad hoc requests for person-identifiable patient information for non-clinical purposes.
- To ensure standard procedures and protocols are in place to govern access to person-identifiable patient information.
- To 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.

Information for Staff

- To ensure standard information governance procedures and protocols are in an understandable format and available to staff.
- To ensure raised awareness, through training and education, of the standards of good information governance practice and Caldicott principles, and that they are understood and adhered to.
- Information Sharing to Support Care
- To work with other care providers and linked agencies to facilitate better sharing of relevant information about patients, in a manner that facilitates joined-up care across institutional boundaries while ensuring that patients' legal rights and the Caldicott Principles are maintained.
- To that end, ensure establishment of Information Sharing Agreements, in line with guidance provided by the Department of Health, to govern the use and sharing of patient-identifiable information between organisations both within and outside the NHS.
- In collaboration with the Information Governance Lead to draw to the attention of all staff through raising general awareness (email bulletins, weekly update, Team Brief and CPD) correct practices in relation to person identifiable patient information, following specific incidents where procedures, guidelines and protocols have been breached by staff.

Strategic

- To ensure that Badger, in its development of strategy and process to implement the various elements of NHS Digital and in compliance with Caldicott Principles and other relevant legislation.
- Specifically, this will include, but not be limited to:
    - Advising on staff registration and authentication processes
    - Assignment of appropriate role profiles to staff
    - Advising on workgroup construction for access control purposes
    - Ensuring that confidentiality alerts and audit trail monitoring are effectively managed
    - To keep abreast of developments within NHS Digital, and in particular the opportunities for safeguarding patient information through promoting the use of anonymised or coded data.

Reporting

- In collaboration with the Information Governance Lead, to draw to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed.
- To raise concerns about any inappropriate uses made of patient information with the Medical Director and/or Chief Executive where necessary.
- On an annual basis, to participate in the NHS Digital DSP Toolkit assessment.
- On an annual basis, to formally report to the Board, Badgers performance against the whole IG agenda making recommendations for further improvement where appropriate

5.1.2 Senior Information Risk Owner

Responsible to: Chief Executive

Job Summary

The Senior Information Risk Owner (SIRO) role will be carried out by the Chief Executive Officer who will take overall ownership of the Organisation's Information Risk Policy, act as champion for information risk and provide written advice to the Badger Board with regard to information risk.

The SIRO will implement and lead the NHS Information Governance (IG) risk assessment and management processes within the Organisation and advise the Board on the effectiveness of information risk management across the Organisation

The SIRO shall receive training as necessary to ensure they remain effective in their role as Senior Information Risk Officer.

Key Responsibilities

Policy and Process

- Oversee the development of an Information Risk Policy. This should include a Strategy for implementing the policy within the existing Information Governance Assurance Framework and be compliant with NHS IG policy, standards and methods.
- Take ownership of the assessment processes for information risk, including prioritisation of risks and review of the annual information risk assessment to support and inform the Statement of Internal Control.
- Ensure that the Board and the Chief Executive Officer are kept up to date and briefed on all information risk issues affecting the organisation and its business partners.
- Review and agree actions in respect of identified information risks.
- Ensure that the Organisation's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
- Provide a focal point for the escalation, resolution and/or discussion of information risk issues.

- Ensure that an effective infrastructure is in place to support the role by developing a simple Information Assurance governance structure, with clear lines of Information Asset ownership and reporting with well-defined roles and responsibilities

Incident Management

- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS IG and DS&P requirements.
- To ensure that there are effective mechanisms in place for reporting and managing Serious Untoward Incidents (SUIs) relating to the information of the Organisation. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learnt.

Leadership

- Provide leadership for Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience, provision of training and creation of information risk reporting structures.
- Advise the Board on the level of Information Risk Management performance within the Organisation, including potential cost reductions and process improvements arising etc.

Training

- The SIRO will be required to undertake information risk management training at least annually to be able to demonstrate their skills and capabilities are up to date and relevant to the needs of the organisation.

5.1.3 Information Governance Lead

Responsible to: Chief Executive Officer

The role of the Information Governance Lead is to coordinate, publicise and monitor the standards of information handling throughout Badger. The role will also include leading on Caldicott, Data Protection and Freedom of Information issues ensuring that employees are fully informed of their own responsibilities for maintaining the standards and that information about the standards is made available to patients where appropriate.

Key Responsibilities

- Ensure that IG is promoted throughout Badger and lead in IG work
- Development of an Information Governance policy and related procedures that satisfies the requirements of the NHS Digital DSP Toolkit.
- Work with other members of the SMT to ensure the development of an Information Governance strategy that sets out the how the IG Policy will be supported in terms of both resources and operationally.
- Ensure that an annual assessment of Badgers performance against the standards in the DSP toolkit is completed, and a plan is in place to enable any improvements.
- Ensure policy and procedures are reviewed according to an agreed schedule and updated where necessary.

Reporting

- Provide when required detailed reports to Senior Management about improvements that have been met, that will be met by years end and those that cannot be achieved without further resource, (personnel or budgetary) and that have already missed the target date.

Profile-raising and Communications

- Raise awareness of the importance of Information Governance throughout Badger and encourage all staff that hold, obtain, record, use and share information to participate in raising IG standards.

Training

- Work with the Training department to ensure all staff complete the Information Governance training programme using Bluestream(Badger corporate training system) and include it as part of induction and ongoing training.
- Maintain and update own knowledge of developments in information management.

Compliance

- Monitor Badger information handling activities to ensure compliance with the legal requirements and internal policy and guidance.
- Assist with investigations into complaints about breaches of confidentiality, Data Protection Act 2018 or Freedom of Information Act 2000 provisions and undertake reporting/remedial action as required. Maintain a log of any incidents and remedial recommendations and actions.
- Provide advice on Information Governance issues.

This list of responsibilities is not exhaustive; the Information Governance Lead will be expected to undertake any other relevant duties appropriate to the grading of the post and requirements of the service.

5.2 Governance

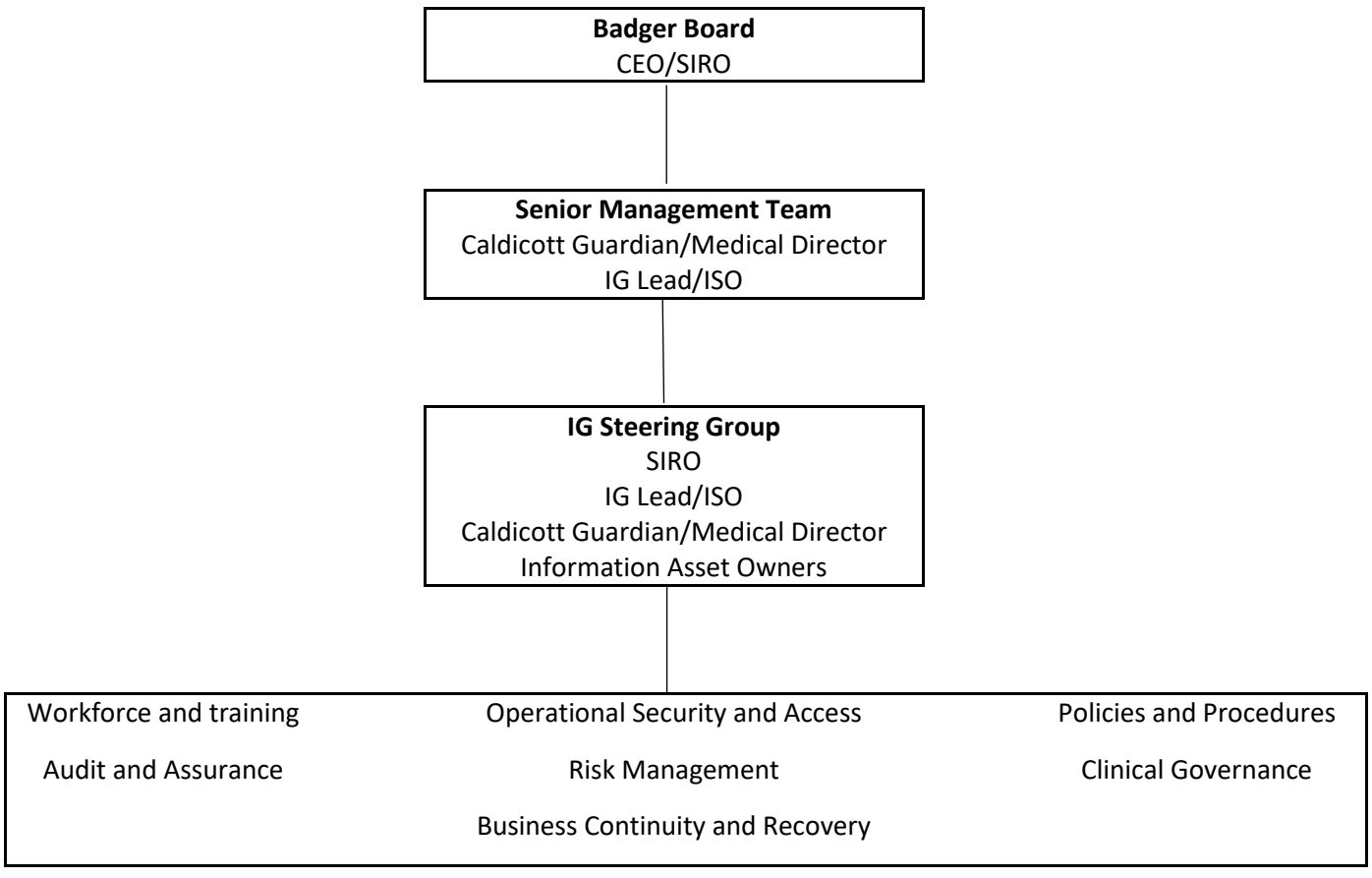
Organisational and managerial structures that support Information Governance issues are essential to properly manage the IG work programme and sustain continual improvements.

To achieve this, the Information Governance Steering Group (IGSG) will coordinate, supervise and direct the work as appropriate to ensure Badger maintains a co-ordinated approach to Information Governance.

5.2.1 Governance Structure

Badger Information Governance Steering Group (IGSG) will take a lead on the implementation of this Framework and related policies and report progress / issues to the CEO and the Executive Team via the Executive Group.

The diagram below reflects the governance hierarchy within the organisation.



5.2.2 Workstreams

Badger workstreams fall within the portfolio of responsibility for members of the Senior Management Team (SMT). The SMT is a functional group that aims to meet weekly to review activities and events across the business and is one of the vehicles to share information quickly and where necessary agree a course of action or seek support.

5.2.3 IG Steering Group

The Information Governance Steering Group (IGSG) is accountable directly to the Badger Board. The purpose of the IGSG is to drive the broader information governance agenda and to provide the Board with the assurance that effective information governance best practice mechanisms are in place within the organisation

The IG Steering Group is responsible for reviewing Badger's management and accountability arrangements for Information Governance, developing and maintaining the IG policy and associated strategy, developing the Information Governance work programme, ensuring that Badger's approach to information handling is communicated to all staff, and monitoring information handling activities to ensure compliance with law and guidance.

Responsibilities

- To review Badger's management and accountability arrangements for Information Governance.
- To develop and maintain the IG policy and associated IG strategy.
- To develop the Badger's Information Governance work programme.
- To ensure that the Badger's approach to information handling is communicated to all staff and made available to the public as deemed appropriate.
- To coordinate the activities of staff given data protection, confidentiality, security, information quality and records management responsibilities.
- To produce reports on the review and the progress, breaches, audits, assurances and related work streams in the IG agenda.
- To monitor the Badger's information handling activities to ensure compliance with law and guidance
- To ensure that training made available by Badger is taken up by staff as necessary to support their role.
- Provide a focal point for the resolution and/or discussion of Information Governance issues.

5.2.4 Badger Board Meeting

The Badger Board meets formally every second month.

The Badger Board is the top level Board across the organisation and the ultimate decision making forum, sharing accountability for the business and compliance needs of the organisation.

The IG Lead produces a reports to the Badger Board for inclusion with Board papers.

5.3 Governance Framework

1. The Information Governance (IG) Lead and SIRO, will be jointly responsible for the annual review of this policy.

2. The IG Lead is responsible for the annual review and implementation of the policy.

3. The IG Lead will:
   - Develop policies, standards, procedures and guidelines;
   - Raise awareness of Information Governance across the organisation;
   - Deal with day to day Information Governance issues;
   - Ensure appropriate training is available to all employees of Badger, and that all mandatory training has been completed

4. Additionally, the following roles will be assigned to key staff to manage the IG agenda
   - Information Asset Owner (IAO)
   - Information Security Officer

   NB as a smaller organisation these are not full time IG positions

5. Badger has established an IG Steering Group to manage the IG agenda, and to ensure that IG is imbedded within Badger's operations.

6. It is the responsibility of all managers to ensure and promote the quality of information and to actively use information in decision-making processes.

7. Minor changes and updates must be submitted to the IGSG for approval, recorded in the IGSG meeting minutes (subject to approval or rejection) and noted in the subsequent quarterly report. Major changes will be agreed by the IG Lead and following approval by the IGSG submitted to the Executive Management Meeting for approval.

8. All directorates across the organisation are responsible for making certain that IG policy and its supporting standards and guidelines are built into local processes ensuring compliance with Information Governance requirements.

9. Non-compliance with information governance policies and procedures may result in disciplinary action up to and including termination of employment or contract

10. All locations and departments within Badger are required to ensure compliance with the information governance policies and procedures outlined in this document, and to provide evidence of compliance during audits and assessments.

11. All employees (permanent, seconded, contractors, graduate management trainees, temporary staff and volunteers) and independent contractors in Badger have individual responsibility to be aware of and conform to the requirements incumbent upon them under this policy in their day to day roles. All employees are responsible for the information, data and records they create and the maintenance of confidentiality and security of them.

12. The roles and responsibilities listed in this document are not exhaustive, and the IG Lead should undertake any relevant duties necessary for the grading of the post and requirements of the service.

13. All directorates and employees at Badger are responsible for ensuring that IG policy and its supporting standards and guidelines are embedded into local processes to ensure compliance with Information Governance requirements.

5.4 Changes

Minor changes and updates to IG policy must be submitted to the IGSG for approval and noted in the subsequent quarterly report. Major changes require approval by the IG Lead and the IGSG.

5.5 Training and Guidance

Badger will:

- Allocate appropriate resources to support the current and evolving IG agenda.
- .
- All staff will undertake annual mandatory online IG training via Bluestream.
- Information is a key component of Induction Training for all staff new to Badger, irrespective of their IG experience prior to joining the organisation. IG forms part of the Mandatory onboarding process and ongoing annual training requirements.

- Employment documentation including the Staff Handbook, Confidentiality Policy and employment terms include the appropriate references to and requirements of adherence to Information Governance covering Data Protection, Confidentiality and compliance for all Data controls.
- Staff are reminded that Information Governance extends to all information, in all forms and across all business areas.

5.6 Dissemination of IG information

All information relating to Information Governance, i.e., policies, procedures and training documentation is available to all staff through the following channels.

Dissemination means	Current Status	Further action required
Adastra – the system which is the core IT system and **used by all** staff at Badger. This is the primary method of information dissemination.	• Up to 90% of staff access Adastra system regularly. • Maintain the IG information on the Adastra communications tab.	• Review and update quarterly, the IG information on the Adastra communications tab. • Utilise the weekly update to identify any new documents, IG campaign materials and helpful reference material.
Pool area on the Shared Server	• All admin and key operational staff have access to the shared pool area. • A new Information Governance directory has been created to hold all IG related documentation	• Ensure all policies are regularly updated and staff notified of relevant changes/updates through the Badger weekly update.
Induction & training materials	• All staff receive induction and mandatory refresher training monitored by the workforce department.	• Ongoing reminders to staff regarding mandatory annual updates.
IG Leaflets & Flyers – Roles and responsibilities	• Leaflets created - quick reference and the role and responsibilities of individuals within Badger	• Include the recently published additions for staff new to IG
IG Awareness Campaign	• Rolling programme of awareness for all staff	• Opportunities for additional items based on feedback and any improvements identified during IG audits and investigations

5.7 Incident Management

Badger has in place a comprehensive incident management policy (CG-02) that spans all Adverse Events including IG Serious Incidents.

CG-02 contains the policy and the procedure to be followed in the event of an incident. Staff are encouraged to complete the incident form enabling management to review the report, assign an owner to investigate and report back on the findings including any action taken and improvements recommended.

All IG Incidents are recorded in the tracker form, reported to the IGSG, Senior Management Team and the Board. Feedback is provided to the person raising the incident and lessons learned applied through process improvement, adherence and reminder of policies, IG campaigns and in the most serious incidents may be dealt with through HR Policies relating to Disciplinary Procedures. In this instance the Workforce Director would be fully engaged to lead on any proceedings.

6 APPENDIX 1 – RELEVANT NATIONAL LEGISLATION

- Records Management Code of Practice for Health and Social Care 20123
- Data Protection Act 2018.
- Freedom of Information Act 2000
- Public Records Act 1958 (updated by the Freedom of Information Act in 2005)
- Access to Health Records Act 1990
- Data Security & Protection Toolkit
- NHS Litigation Authority Risk Management Standards
- Care Quality Commission Standards
- Information Security Management: NHS Code of Practice
- Confidentiality: NHS Code of Practice
- The Caldicott Principles 2020
- General Data Protection Regulations

Badger will review and update this policy as necessary to ensure compliance with any future changes to national legislation regarding information governance.