Legislation

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'. They must make sure the information is: • Used fairly, lawfully and transparently

- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited only to what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Badger and our staff provide and manage what is known under GDPR as 'special category data' requiring extra protection.

Privacy Policy

Under GDPR Badger needs to make our Privacy Policy public and this is shared on our website and notices directing patients to it's location are within each Primary Care Centre.

Under the Data Protection Act 2018, everyone has a right to see the information held about them (Subject Access Request). To do this, they have to meet certain criteria. To find out more, contact the IG Lead.

Human Rights Act 1998

Article 8: Everyone has the right to respect his/her private and family life, home and correspondence. It is unlawful for a public authority to act in a way that is incompatible with a Convention right.

Common Law Duty of Confidence

Information obtained for one purpose should not be used for another purpose without the express or implied authorisation (consent) of the provider of that information.

The Freedom of Information Act (FOI)

The FOI gives the public the right to request non-personal information from a public authority. As Badger is not a public authority, we do not have to respond to such request; however, indirect request may come via the CCGs. For further information, contact IG Lead, or Caldicott Guardian.

Records Management Code of Practice for Health and Social Care 2016

All staff have a legal and professional obligation to be responsible for any records they create or use in the performance of their duties. Any record created by an individual, up to the end of its retention period, is a public record and subject to Information requests.

All information should be accurate, up to date, complete (including NHS Number), quick and easy to find and not duplicated.

Data Security & Protection Training

The HR team will arrange for the appropriate training. Please contact HR for support.

Where to find more details

The latest Badger Information Governance and Data Security and Protection Policies and Guidance Leaflets are available on Adastra, Team Leader Desk and the shared pool area.

Reporting an Incident

Form IG-08-F1 is to be used for reporting all IG Serious Untoward Incidents (actual and potential).

For further Information contact the IG Lead

We understand that you might be anxious about any requests for data and how you should manage that. Please follow the guidance that directs a patient to complete a form which will then be managed by the Governance Team at Badger House.

The most important thing you can do is protect all data whether it belongs to a patient, a colleague or relates to the business as if it was your own.

Author	Date	Ver	Ref	Issue Date	Next Review
A Savage	April '23	V7.0	IG-18	April '23	April '26

badger
CARE YOU CAN TRUST

Data Security and Protection and Information Governance

Understand your responsibilities

Key Contacts

Caldicott Guardian	**Dr. Fay Wilson**
Senior Information Risk Owner	**Dr Waqar Azmi**
IG Lead	**Andrew Savage**
IG Training	**Training Team**

Introduction

All employees of Badger are responsible for maintaining confidentiality. This duty of confidentiality is written into employment contracts. A breach of confidentiality relating to information gained, either directly or indirectly in the course of duty is a disciplinary offence that could result in dismissal.

Staff are authorised to have access to patient information in order to perform their duties. Accessing or attempting to gain access to information that you do not need to see to carry out your work is a breach of confidentiality. Passing information on to someone who is not authorised to receive it is also a breach.

Any personally identifiable information (PII), non-clinical or clinical, must be treated as confidential. The general principles underlying the use and sharing of personal information should follow the Caldicott Principles:

- Justify the purpose for using patient confidential information.
- Only use patient identifiable information when absolutely necessary.
- Use the minimum identifiable information required for this purpose.
- Access should be on a strict need-to-know basis only.
- Everyone must understand their responsibilities to protect information.
- Everyone must understand and comply with the Law.

Requests for Information

If a patient or their representative request information about their case you must advise them to put their request in writing to qualityandcompliance@badger.nhs.uk or
Quality and Compliance, Badger House, 121
Glover Street, Birmingham, B9 4EY

Basic Principles

Any personal information given for one purpose must not be used for another purpose without the consent of the individual concerned because that use may breach confidentiality.

A patient's right to confidentiality is protected by ethics and the Law.

Patients have a legal right to know what information is being collected and for what purpose information is being shared. In some circumstances, they have a right to restrict and withhold the use of personal data.
Every member of staff has an obligation to protect confidentiality and a duty to verify the authorisation of another person to ensure information is only passed on to those who have a right to see it.

All staff should understand their responsibility to protect the confidential information they collect and use by following the rules and guidance that are available to them.

The rules are there to protect both the patient and staff from breaches of confidentiality.

You are responsible for your decision to pass on information.

If you are unsure about whether or not to disclose information, consult your Line Manager and/or, if necessary, obtain advice from Badger's Caldicott Guardian, Dr Fay Wilson

Duty of Care

All reasonable care should be taken to protect the physical security of confidential information from accidental loss, damage, destruction, unauthorised access or accidental disclosure.

For example:
Do not share your username(s) and password(s) with anyone.

- Confidential data held on computers, laptops, disks or memory sticks should be kept physically secure, password protected and encrypted.
- All transfers of personal identifiable data electronically outside of Badger must be pre-authorised and encrypted unless all personal identifiers are removed.
- Patient information should be kept secure and not left unattended for the patient or public to see.
- Faxing is a less secure method of sending confidential information and this should only be used following the Safe Haven Policy, following authorisation and via a secure fax machine.
- Envelopes containing patient/staff confidential information must be securely sealed, labelled "Confidential" and clearly addressed to a known contact.
- Telephone validation procedures must be followed to confirm the identity of telephone callers before information is given to them.
- Follow Badger's Information Security and Information Governance policies and procedures and seek advice when in doubt.