CONFIDENTIALITY POLICY

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

Destroy All Previous Issues

Contents

DOCUMENT CONTROL

Document Storage

Location: p:\ops team\central policies & procedures - development - word docs\it policies\it-po-01 confidentiality policy v1.0.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
V1.0	July 2022	Doc Control	Original version was previously HR-09 (HR Policies) it was agreed this should come under IT with immediate effect
V1.1	July 2022	Andrew Savage	Policy updated to reflect current UK acts and GDPR legislation

Approval

Version	Name	Position	Signature	Approved Date
V1.1	Badger Executive	Executive Team	Exec Team	17/08/2022 (Sent via email for approval 11.08.22)

Glossary

Term	Description
DPA	Data Protection Act
GDPR	General Data Protection Regulation

1 INTRODUCTION

This paper outlines the policy on confidentiality at Badger and seeks to meet the requirements of the relevant legislation, predominantly:

- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Data Protection Act 2018 - UK's implementation of the General Data Protection Regulation (GDPR)
- The Common Law of Confidentiality

Everyone working for Badger is under a legal duty of confidentiality and this policy has been implemented in order to protect staff and patients by ensuring that all employees have access to information advising on the correct procedures to be adhered to.

Badger provides a training session on confidentiality and child protection. However, if staff cannot attend these training sessions during their induction period, it is their responsibility to ensure they do attend a training session so that they understand and comply with the law on confidentiality. To attend training sessions staff should contact their line manager for details.

2 SCOPE

This policy applies to all staff, working in the organisation. It also includes, but is not limited to, Executive and Non-Executive Directors; self employed Doctors, students, volunteers, staff of other organisations and external contractors who can access personally identifiable information. It applies to all handling (processing) activities (i.e. the holding, obtaining, recording, using, sharing, deletion/ destruction) involving personally identifiable (confidential) information.

This policy equally applies to any sensitive corporate information regarding Badger's business affairs that fall outside its duty of openness within the terms of the Data Protection Act 2018, and the organisation's commitment to openness regarding the purpose and processing of all patient identifiable information.

3 WHAT INFORMATION IS CONFIDENTIAL?

Confidential information can be anything that relates to patients and staff (including non-contract, agency staff or locums, their family or friends, or Badger's confidential corporate information however stored).

Information (hard copy, electronic or tacit) may be held on paper, computer file, video, photograph or even in the memory of an individual. It includes information stored on portable devices such as laptops, tablets, memory-sticks, mobile or smart- phones and digital cameras.

It can take many forms including medical notes, audits, employee records including payroll, occupational health records etc. Personally identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number, photograph or any other form of identification.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

4 KEY LEGISLATION

4.1 Human Rights Act 1998

Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their employment and health records.

Current understanding is that compliance with the Data Protection Act 2018 and the Common Law of Confidentiality should satisfy Human Rights requirements. Legislation generally must also be compatible with the HRA98, so any proposal for setting aside obligations of confidentiality through legislation must pursue a legitimate aim; be considered necessary in a democratic society and be proportionate to the need.

4.2 The Computer Misuse Act 1990

This Act is relevant to electronic records and data and creates three offences of unlawfully gaining access to computer programmes.

- Unauthorised access to computer material
- Unauthorised access with intent to commit or cause commission of further offences
- Unauthorised modification of material

It is therefore essential that staff ensure they have the appropriate rights to access any information held on Badger computers or any electronic information related to the organisation that is held, or accessible from elsewhere.

4.3 Health and Social Care Act 2012: Section 60 - Co-operation with bodies exercising functions in relation to public health

Section 60 of the Act creates a power for the Secretary of State to make orders (subject to various safeguards) requiring the disclosure of patient data that would otherwise be prevented by a duty of confidence.

The Health Service (Control of Patient Information) Regulations 2002 were the first regulations to be made under section 60 of this Act and support the operations of cancer patient's registries and the Public Health Laboratory Services in respect of communicable diseases and other risks to public health.

4.4 The Data Protection Act – 2018

The Data Protection Act 2018 is the UK's implementation of the **General Data Protection Regulation** (GDPR)

The DPA 2018 became effective from 1st May 2018 and superseded the DPA 1998 and Access to Health Records Act 1990. The exception to this is the records of deceased persons, which are still governed by the Access to Health Records Act.

Within the DPA 2018 a health record is defined as a record consisting of information about the physical or mental health or condition of an identifiable individual made by, or on behalf of, a health professional in connection with the care of that individual.

A health record can be recorded in a computerised form or in a manual form. Badger may include such things as, hand-

written clinical notes, letters to and from other health professionals, laboratory reports, videos and recordings of telephone conversations.

The DPA 2018 is not confined to health records held for the purposes of the National Health Service. It applies equally to the private health sector and to health professionals and private practice records.

This Act also provides a framework that governs the processing of information that identifies living individuals - personal data. The DPA imposes constraints on the processing of personal information in relation to living individuals. It identifies data principles that set out standards for information handling.

4.5 Common Law Confidentiality

Common Law is not written as an Act of Parliament like the Human Rights Act but, it is a law that is built up from case law. This means that the law has been established by individual cases and judgements over several years.

The general position of common law is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient.

4.6 Access to Health Records under Data Protection Act 2018

The Principles of the DPA

- Information should be obtained and processed fairly and lawfully.
- Personal data shall be held only for one or more specified and lawful purposes.
- Personal data held for any purpose shall not be used or disclosed in a matter incompatible with that purpose.
- Personal data for any purpose shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data held for any purpose shall not be held for any longer than is necessary for that purpose or those purposes.
- An individual shall be entitled:
  i) At reasonable intervals and without undue delay or expense
     1. To be informed by any data user whether they hold personal data of which the individual is the subject, and
     2. To have access to any such data user, and
  ii) Where appropriate to have such data corrected or erased.

Appropriate security measures shall be taken against unauthorised access to, alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.

5 EMPLOYEE OBLIGATIONS

Badger employees are under a contractual obligation of confidence and staff are aware of the confidential status of the information which will bind the receiver of information to confidence.

If health professionals are found to be in breach of confidence their professional bodies will be advised.

The unauthorised passing on, or use of patient information by a staff member in the absence of an overriding public interest justification (see IG-22 – Access to Records Policy and Procedure and Disclosure in the Public Interest below), is likely to be unlawful and may result in disciplinary action leading to dismissal.

Furthermore, legal action against Badger, and/or the individual involved in the disclosure may result from a breach of confidence.

6 ABUSE OF PRIVILEGE

It is strictly forbidden for employees to look at any information relating to their own family, friends, acquaintances, or employees unless they are directly involved in the patient's clinical care or with the employee's administration on behalf of Badger.

Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action leading to dismissal. If you have concerns about this issue please discuss with your line manager.

7 CARELESSNESS

Any breach of confidence resulting from employee carelessness may result in the same disciplinary action being taken as with any other confidence breach.

In order to avoid any such inadvertent disclosure, employees should consult the following best practice guidelines:

- Do not talk about patients in public places or where you can be overheard.
- Do not leave any medical records or confidential information lying around unattended.
- Make sure that any computer screens, or other displays of information, cannot be seen by the general public.
- Do not share passwords with other members of staff and do not leave your logon id and/or password written down and left on the desk or fixed on the side of the computer.
- Ensure the physical security of the building is not breached. Lock all doors, windows and lockable filing cabinets when leaving the building.
- Wherever possible individuals should adopt a **clear desk and clear screen policy** to reduce the risk of unauthorised access or loss or damage to sensitive information outside normal working hours or when areas are unattended. Information left on desks is also likely to be damaged or destroyed in a disaster such as fire, flood, or explosion.

8 VISITORS

A member of staff at supervisor or manager level must accompany visitors whilst on the site.

Prior agreement must be obtained from the Caldicott Guardian prior to any photographs being taken within the call

centre or primary care centres.

9 RESPONSIBILITY TO GENERATE ANONYMISED & AGGREGATED INFORMATION

Under the Terms of the Confidentiality and Disclosure of Information Code of Practice (2005), guidance is given that, wherever practicable, patient data disclosed for purposes other than the patient's care should be anonymised.

Anonymised Information is information that does not identify an individual. Anonymised or statistical information is not confidential and may be used with relatively few constraints.

Anonymisation requires the removal of name, address, full postcode, date of birth, NHS number and local patient identifiable codes, and any other detail or combination of details that might support identification.

Aggregated Information is statistical information, which if care is taken with respect to rare conditions etc, will also provide anonymity for patients.

In certain circumstances, the organisation may need to anonymise patient records prior to disclosure. It will usually be for the staff member passing on the data to ensure that it is passed on in a non-identifiable form, wherever that is practical.

Badger is committed to developing the organisation's capacity to generate anonymised and aggregated information. In particular, the upgrading of IT equipment will provide opportunities to improve this capacity.

There are circumstances where it will not be practicable for anonymised information to be generated in order to satisfy the purpose of third parties. This may be because there is limited capacity to anonymise information, or where the organisation is unable to anonymise data with a reasonable degree of ease, for example, because it would involve substantial additional work, or because the purpose to be satisfied requires examination of original records. Where any of these apply, care must be taken to ensure that any disclosure of information remains lawful.

10 COMMUNICATIONS

10.1 Telephone Calls

10.1.1 Identifying inquirers, so that information is only shared with the right people. Staff should check that any callers, by telephone or in person, are who they say they are.

10.1.2 There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. Seek official identification or check identity before calling back (using an independent source for the phone number). Check also that they have a legitimate right to have access to that information.

10.2 Answer Machine/Voicemail

10.2.1 Messages about appointments should only be given directly to patients or to their legal guardians or carers. Unless you have the *explicit* consent of the patient to leave a full message on an answer phone (i.e. you have

ensured that you have the correct number and the patient does not mind if someone else hears what you will say) you should only leave the minimum information, or call back later.

If you have to leave a message and you do not have consent, you should say:

- Who you are
- What your number is

You should not say:

- Where you are calling from
- What the message is about

10.2.2 Leaving a message at a person's workplace, that lets a work colleague know that they are attending a particular clinic, could compromise confidentiality. If you are asked what it is in connection with, for instance if you have to leave a message at someone's place of work, staff are advised to say that it is a confidential matter.

10.2.3 Messages about children above the age of self-determination (see policy IG-22 – Access to Records Policy and Procedures) should not be given to parents (e.g. Mums ringing on behalf of students), nor should messages be given to spouses, unless you are *certain* that you have the consent of the patient. This can cause some difficulties; people may complain that you are being obstructive, or perhaps spouses may suspect that there is more than a hospital appointment being planned.

10.2.4 If you must give a message to someone other than the patient, for instance if the patient is unable to answer for themselves, or cannot hear over the telephone, you must make efforts to ensure that the patient consents to the information being given to the other person, e.g. by asking if the patient is there with them.

10.2.5 Where people call back and the telephone is answered using the name of the organisation, this can be seen as a *de facto* admission that the patient has some connection with Badger, however it is preferable to leaving the location with the original message.

10.3 Mail

10.3.1 This means personal information/data should be addressed to a person, a post holder, a consultant or a location known to be secure, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader.

10.3.2 Mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate.

10.3.3 External Mail must also observe these rules. Special care should be taken with personal information sent in quantity, such as collections of patient records on paper or other media.

10.3.4 These should be sent by Recorded Delivery or by courier, to safeguard these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor.

10.4 Faxing

10.4.1 Patient identifiable data should be removed from any faxes unless directly related to the purpose for faxing.

10.4.2 Faxes should always be addressed to named recipients and should only be forwarded to trusted fax numbers such as those recorded on the adastra system.

10.4.3 Always check the number to avoid misdialling and where no fax report is available, ring the recipient to check that they have received the fax.

10.4.4 If the fax machine stores numbers in memory, always check that the number held is correct and current before sending sensitive information.

10.5 Email

10.5.1 Do not forward a confidential message without acquiring permission from the sender first

10.5.2 Email is an insecure system. Therefore sensitive personal/health information (i.e. that relating to identifiable individuals) or commercially sensitive information MUST NOT be sent by email unless it is encrypted to the NHS standards, NHSmail must be used,

10.5.3 If you unlawfully forward confidential information, you and the Organisation can be held liable

11 MEMORY STICKS

No patient or employee details must be downloaded on to memory sticks or transportable devices without prior agreement with the Chief Executive. Where approval is given any information must be encrypted and protected to ensure no unauthorised access is possible.

Any such information must be destroyed once it is no longer required for the purpose for which approval was granted

12 DISCLOSURE TO THIRD PARTIES OR OTHER BADGER EMPLOYEES

12.1.1 Occasions do arise where it does become necessary to breach confidentiality and these are discussed during Confidentiality training. These situations will include:

- Patient's consent;
- Other health professionals involved with the patient's care – may still require the patient's consent;
- In the patient's best interest e.g. patient/public safety
- If a court order has been received to provide confidential information in a court of law;
- If the police require access to records they must provide a warrant that has been issued by a *circuit* judge;
- Bodies concerned with health administration such as Department of Health, Coroner, Health Service Ombudsman;
- In the public interest;
- Acts of Parliament e.g. Control of Diseases Act 1984; The Children Act 2004 makes it a duty to share information about child abuse.
- Research that has been approved by an ethical research committee.

12.1.2 Reference should be made to IG-22 – Access to Records Policy and Procedure; this document gives clear details and procedures to follow if a request to release information is received.

12.1.3 It must be emphasised that issues regarding confidentiality are complex in nature. Before a decision is made to disclose any information, it must first be discussed with the senior line manager, the Patient Services Manager and/or the Caldicott Guardian.

12.1.4 In certain circumstances legal advice should be sought. Employees should be aware that a decision to disclose information without consent, if challenged, may need to be defended in the High Court. It is therefore imperative that appropriate records are made at the time of disclosure.

12.1.5 ***If a disclosure is made which is not permitted under Common Law the patient can bring legal action not only against the organisation but also against the individual responsible***

12.1.6 Never give out information on patients or staff to persons who do not "need to know" in order to provide health care and treatment.

- Always check the member of staff is who they say they are
- This can be achieved by checking the employee's ID badge and/or their internal extension number prior to giving them any information
- If possible also check whether they are entitled to the information
- Don't be bullied into giving out information

- If in doubt, check with your line manager.

12.2 Patient Requesting Non Disclosure to their GP

12.2.1 In the event that a patient specifically requests that they do not want their medical notes to be sent to their GP, the patient must discuss this with a Badger doctor.

12.2.2 Only a doctor can ultimately make a decision on whether it is clinically necessary for the patient's own GP to be informed of the contact with Badger. A doctor must explain the clinical risks to the patient and the rationale for the disclosure and ensure that this is recorded on the patient's medical notes.

12.2.3 It is essential under the terms of fair processing of data set out in the DPA, that Badger staff make patients aware that the information the organisation collects is routinely forwarded to their own GP.

12.3 Access to Health Records

12.3.1 Under the terms of the Data Protection Act 2018 individuals have a legal right to seek access to their records; and in some cases, applications may be made by individuals seeking access to another person's health record; however there are a number of considerations which may either restrict or prohibit such access.

12.3.2 It is therefore paramount that all employees fully understand their duties under the law, guidance to which is given in the central policy: IG-22 - Access to Records Policy and Procedure, but any proposed disclosure should be referred to the patient services manager (PSM).

12.4 Disclosure 'In the Public Interest'/ to Protect the Public

12.4.1 Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of confidential service.

According to The Public Interest Disclosure Act 2018 disclosures qualifying for protection tend to show one or more of the following:

a) that a criminal offence has been committed, is being committed, or is likely to be committed,

b) that a person has failed, is failing, or is likely to fail to comply with any legal obligation to which he is subject,

c) that a miscarriage of justice has occurred, is occurring, or is likely to occur,

d) that the health or safety of any individual has been, is being or is likely to be endangered,

e) that the environment has been, is being, or is likely to be damaged, or

f) that information tending to show any matter falling within any one of the preceding paragraphs has been, is being, or is likely to be deliberately concealed.

It makes no difference whether the circumstance leading to the breach is within or outside of the UK, as long as either UK law or the law of other jurisdiction prohibits it.

12.5 Serious Crime and National Security

12.5.1 The definition of serious crime is not entirely clear. Murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm may all warrant breaching confidentiality.

12.5.2 Serious harm to the security of the state or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

12.6 Risk of Harm

12.6.1 Disclosures to prevent serious harm or abuse also warrant breach of confidence. The risk of child abuse or neglect, assault, a traffic accident or the spread of an infectious disease are perhaps the most common that staff may face.

12.6.2 However, consideration of harm should also inform decisions about disclosure in relation to crime. Serious fraud or theft involving Badger or NHS resources would be likely to harm individuals waiting for treatment. A comparatively minor prescription fraud may actually be linked to serious harm if prescriptions for controlled drugs are being forged.

12.6.3 It is also important to consider the impact of harm or neglect from the point of view of the victim(s) and to take account of psychological as well as physical damage. For example, the psychological impact of child abuse or neglect may harm siblings who know of it in addition to the child concerned.

12.7 Other Disclosures in the Public Interest

12.7.1 Similarly, when the public good that would be served by disclosure is significant, there may be grounds for disclosure. The key principle to apply here is that of proportionality. Whilst it would not be reasonable and proportionate to disclose confidential patient information to a researcher where patient consent could be sought, if it is not practicable to locate a patient without unreasonable effort and the likelihood of detriment to the patient is negligible, disclosure to support the research might be proportionate. Other factors e.g. ethical approval, servicing and safeguards, anonymisation of records and or clear deletion policies etc might also influence a decision on what is proportionate. It is important not to equate "the public interest" with what may be "of interest" to the public.

12.8 How a Public Interest Disclosure Should be Made

A record must be made of any such circumstances, so that there is clear evidence of the reasoning used and the circumstances prevailing.

12.8.1 Whoever authorises disclosure must make the record; this would normally be the Patient Services Manager.

12.8.2 Disclosures in the public interest should also be proportionate and be limited to relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies and a clear record of the decision making process and the advice sought is in the interest of both staff and the organisation.

12.8.3 Wherever possible the issue of disclosure should be discussed with the individual concerned and consent sought. Where this is not forthcoming, the individual should be told of any decision to disclose against their wishes. This will not be possible in certain circumstances, e.g. where the likelihood of a violent response is

significant or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt investigation.

A qualifying disclosure must only be made:

- In good faith to the individual's employer, or to any other person having legal responsibility for the conduct complained of;
- For the purpose of obtaining legal advice;
- Where the worker is employed by the crown, in good faith to a Minister of the Crown; or
- In good faith to a person prescribed by the Secretary of State

Under this Act, the worker must reasonably believe that any allegation he makes is substantially true.

If it is the employer who is responsible for the conduct complained of, the Act allows a worker to make a disclosure to a person not noted above, provided the following conditions are met:

- It must be made in good faith, and not for personal gain, with a reasonable belief that the allegations complained of are true; and
- The worker reasonably believes he will suffer a detriment if he makes the disclosure to his employer; or
- He has previously complained of the conduct and no action has been taken; or
- He reasonably believes that evidence of the conduct has been or will be destroyed or concealed.

Such a disclosure will be subject to a test of reasonableness, which is tested with reference to:

- The person the disclosure was made to;
- The seriousness of the conduct complained of;
- Whether the conduct is continuing;
- Whether any previously made complaint was acted upon; and
- Whether the worker followed any procedure laid down by the employer.

12.8.4 Each case must be considered on its merits. Decisions will sometimes be finely balanced and staff may find it difficult to make a judgement. It may be necessary to seek legal advice (e.g. from professional, regulatory or indemnifying bodies) or await to seek a court order. Staff need to know who and where to turn to for advice in such circumstances.

12.9 Freedom of Information – Access to Corporate Information

12.9.1 Due to the nature of Badger's relationship with the NHS, from time to time employees may receive requests for information from both individuals and business under the Freedom of Information Act 2000 (FOIA).

12.9.2 As a private Organisation, Badger *does not* fall under the jurisdiction of the FOIA and therefore is under no legal obligation to openness concerning its corporate practices under the Act.

12.9.3 This does not affect the organisation's responsibilities or commitment to the DPA which requires openness regarding what patient and staff information will be collected by Badger and how that information will be used and processed.

12.10CCG Access to Anonymised Information

12.10.1 CCGs may require access to anonymised patient information for a range of purposes. Where CCGs require access, they should explain the precise purpose for which access is needed and who will gain access. These circumstances include:

- Strategic Planning
- Financial Management
- Public Health
- Workforce Planning
- To check that payments under the Quality and Outcomes framework (QOF) are, or have been, accurate, complete and correct.
- To carry out an annual review of the contractor's performance, including patient experience, against the QOF.
- Clinical audit purposes
- Internal audit
- To deter, prevent and detect fraud
- Where the CCG has concerns about a contractor's compliance with its contract

12.10.2 Whilst anonymised information, if properly processed, is not subject to the restrictions of confidential patient information, a person acting on behalf of the CCG must, if requested, produce written authorisation to the organisation in order to see or access Badger data.