THE WATERLOO PRACTICE

Data Protection and Confidentiality Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1	30.04.21	N Siswick	All Partners	New version following restructure
2	01.05.22	N Siswick	All Partners	Change to wording re SAR of deceased patients, no longer passed to PCSE.

Section **Page**

Document Summary Table
Contents

Appendices

1. Introduction

The aim of this Policy is to ensure that all practice staff including locum, temporary and those staff supplied by external organisations are aware of their responsibilities for the use of patient and staff information. It is based on the Confidentiality NHS Code of Practice and the General Medical Council (GMC) Confidentiality: good practice in handling patient information

This document is not as wide-ranging as those that it is based on, nor is it intended to be. Should any member of staff have any concerns regarding confidentiality, then in the first instance they should approach the Practice Manager. If the Practice Manager is unable to resolve the query, then the Practice Manager should contact The Health Informatics Service (THIS) on 0845 1272600 who will be able to offer more specialist advice.

2. Common Law Duty of Confidence

All NHS bodies and those carrying out functions on behalf of the NHS have a common law duty of confidentiality to patients and a duty to maintain professional ethical standards of confidentiality.

Data Protection Act 2018 / General Data Protection Regulations

The Data Protection Act 2018 is the legislation that governs the use of personal identifiable information in any format including but not limited to computer records, paper records, photographs and video recordings. The Act only applies to living individuals

The Act places several responsibilities on the Practice (known as the principles). These are listed and explained in Annex A of this policy. The Act also gives the individual to whom the information relates certain rights, shown in Annex B the main one as far as the practice is concerned is Subject Access Request. Specific guidance on how to handle a request from an individual or their representative (e.g. solicitor) to view their records is given in Annex C.

The Access to Health Records Act 1990 was superseded by the Data Protection Act but remains in force for access to the records of the deceased. Details of who may access the records of the deceased are given in Annex D.

Caldicott Report

The Caldicott Committee, Chaired by Dame Fiona Caldicott, was set up by the Chief Medical Officer in 1997 following increasing concerns regarding the way patient information flowed, not only within NHS organisations, but also to and from non-NHS organisations.

The Report made sixteen recommendations. One of the recommendations was the appointment of a Caldicott Guardian, who should be a senior health professional or an existing member of the management board, for each organisation.

The Guardian is responsible for agreeing and reviewing protocols for governing the disclosure of patient identifiable information across organisational boundaries.

All NHS organisations, local authorities which provide social services must have a Caldicott Guardian.

Our Caldicott Guardian is Dr Farooq Hameed.

The Committee also initially developed a set of 6 general principles for the safe handling of patient identifiable information and these Principles are the guidelines to which the NHS works. A seventh principle was added in 2013 and an eighth in 2020

The Caldicott Principles-

i. Justify the purpose.
ii. Don't use patient identifiable information unless it is absolutely necessary.
iii. Use the minimum necessary patient identifiable information.
iv. Access to patient identifiable information should be on a strict need to know basis
v. Everyone should be aware of their responsibilities
vi. Understand and comply with the law
vii The duty to share information can be as important as the duty to protect patient confidentiality
viii Inform patients and service users about how their confidential information is used

Patient Confidentiality

All information held in a patient's record is private and confidential.

Patients have an expectation that any information that passes between them and a health professional will remain confidential. If this trust is not maintained, then patients may feel reluctant to pass on information to the health professional which may impact on their treatment.

As part of their treatment the patient understands and expects that information about them must be shared. However, patients generally have the right to object to the use and disclosure of confidential information that identifies them, and they need to be made aware of this right.

Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment.

Patients do realise that non-clinical staff may become aware of information relating to their health as the result of carrying out administrative functions within the practice.

Except for health professionals, the main contact that a patient has with practice staff are the Reception Patient Advisors. This, therefore, places special obligations and responsibilities on Reception Patient Advisors.

- Reception Patient Advisors should not ask why a patient wishes to see a Health Professional, unless the patient has been made aware of this prior to being asked, this may either be signage or a pre-recorded telephone message
- If a patient volunteers the information that is perfectly acceptable, but the patient must not feel under any pressure that they must disclose why they wish to see a health professional.

- Reception Patient Advisors must be aware of the danger of discussing personal information with a patient, even changes of address at reception, where they can be overheard.
- Reception Patient Advisors should offer patients the opportunity to speak privately if the patient so wishes.
- If a patient attends the reception with an interpreter, then staff must make a record of this. If you have any concerns about the information that is being requested via the interpreter, you must contact the Practice Management Team immediately before disclosing any information.

Children

Fraser Guidelines / Gillick Competence
This allows a person under the age of 16 to be seen by a health professional without the knowledge or consent of their parents, regardless of what the treatment is.

Fraser Guidelines are specific to contraception, sexually transmitted infections and pregnancy. Whereas Gillick Competence refers to wider health matters

No person in the practice other than a health professional may decide if a child is Fraser / Gillick competent.
-
For a child to be deemed Fraser / Gillick Competent the following criteria **must** be met: -

- The child must fully understand the nature of the treatment.
- The child must fully understand the outcomes of any treatment.
- The child must be encouraged to involve their parent(s) or another responsible adult who they trust, if it is not practicable to involve their parent(s) (Possibly a teacher)
- For Fraser, the child would continue to be sexually active, with or without contraception
- Unless he or she receives treatment/contraception their physical or mental health (or both) is likely to suffer.
- The young person's best interests require contraceptive advice, treatment or supplies to be given without parental consent.

3. Subject Access

Patients accessing their records on line
If a patient wishes to access their records online, then the same precautions are to be taken, prior to access being granted, as if you were supplying the patient or their representative i.e. solicitor with a copy of the record – See Annex C for this procedure

All Staff

- If a patient contacts the practice, they should be asked for their personal & demographic information, which must match the information held on the clinical system, before any personal information is divulged.
- Information in a patient's record can only be discussed or passed on to the patient personally, unless the patient has given their explicit consent that another person maybe informed except in exceptional circumstances

- If any information is requested about a patient by any other person or agency i.e. police, employer, insurance company etc. It must be referred to the Practice Management Team.
- You should never confirm or deny the presence of a patient at the practice unless you have the patient's express permission to do so.
- All computer screens should be positioned in such a manner that they cannot be read by members of the public.
- You must **NEVER** disclose your computer login password to anyone
- You must **NEVER** share your smart card with anyone nor must you leave your smartcard unattended.
- Only health professionals are qualified to inform patients of test results. You must not inform anyone of a test result unless the health professional has given their express permission that you may do so; this includes the results for your family and friends.
- Staff must not look up their own health care records, if they are registered at the practice or those of any other person if they are not involved in the provision of care for that person. Even if staff have a close personal relationship with patients e.g. friends or family - and even if the friend or family member has given them consent to look at their records), staff must still not look up these records for any purpose whatsoever, for example, to view test results or confirm appointments
- Staff should be aware that the practice has the ability to monitor and see what records and other information, a member of staff may have accessed.
- If information about a patient is requested by another healthcare provider via telephone i.e. a hospital, you must verify that the person has been referred to that hospital. If it is a request from an Accident and Emergency unit it should be referred to an appropriate health professional. Once it has been established that the healthcare provider has a legitimate right to the information, they should be telephoned back immediately. You must validate any telephone number given independently and it should always be to a landline. If you have any doubts as to the authenticity of a telephone number, you should go through that organisation's switchboard.
- You must never leave any medical information on a patient's telephone answer machine, however it acceptable to leave a message asking the patient to call the surgery.
- Children who are deemed to be competent are due the same level of confidentiality as an adult.
- It is the responsibility of all members of the practice team to be aware that personal information about patients should not be discussed in areas where conversations can be overheard by members of the public (i.e. patients in the waiting room or queuing at the reception).
- Information regarding patients **must never** be discussed outside of the work environment. If **any** member of staff discusses patient information even with a colleague outside of the work environment it will be considered as gross misconduct and is of sufficient severity to be regarded as terminating or justifying the termination of the contract of employment, and or notifying the appropriate regulatory body. As stated in the Terms and Conditions of Employment the right is reserved for instant dismissal in such a case of gross misconduct.

4. Communicating Information – Telephone, Faxing, Texting, Removable media and Email

No method of communication can be 100% secure so staff should take care in whatever medium of communication they use.

- Staff should be aware of who they are talking to on the telephone and if they are requested to telephone someone back they should always verify any telephone numbers independently.
- Fax - The Department of Health & Social Care mandated that faxing should cease from 1 April 2020. If patient information is to be faxed then the information should be faxed to a safe haven. If the member of staff is uncertain if the fax has been designated as safe haven then they should telephone the person that they are wishing to fax the information too and verify fax number and confirm receipt of the fax. A confirmation that the fax has been delivered must be obtained
- Email, if you are emailing identifiable information then it must be encrypted to 256 Advanced Encryption Standard (AES). Most email systems now offer encryption, if you are unsure then contact THIS on 0845 1272600
- If any information is to be sent or stored on any type of portable storage device, such as a memory stick or DVD, then the GMC state that the information must be encrypted to approved NHS standards which is currently 256 AES If information is to be sent or stored on unencrypted media, then the reason must be documented.
- If a patient has supplied their mobile telephone number, then it is acceptable to text patients to remind patients of any upcoming appointments. There is no requirement to obtain explicit consent to text patients. Text message's must not contain any information that can clearly identify the patient, if it is accidently sent to the wrong telephone number or it is a shared phone
- Increasingly patients are wishing to communicate with the practice via email. If the practice wishes to receive incoming emails, then they must set up specific email accounts
- Any such email account must have appropriate automatic reply
- If the patient has explicitly stated they wish to receive information by email, even if it is unencrypted, then this is acceptable, so long as the risks are explained to the patient such as a shared family computer or smart device.

Incorrect Information

- Under the Data Protection Act all information must be accurate and up to date. Staff should regularly ask patients if their basic information is correct i.e. telephone number, address etc.
- If a change of address is requested, proof of the new address should be requested, such as a Council Tax bill, confirmation of post redirection from Royal Mail, unless someone at the practice can vouch for the individual's identity.
- If a patient feels information medical information recorded in their health record is factually incorrect then they should firstly make an informal approach to the health professional concerned to discuss the situation in an attempt to have the records amended.
- The patient should produce evidence to support their claim that the record is factually incorrect. If they produce such evidence, then the record can be corrected or amended.
- If the patient cannot provide evidence to support their claim, then they may request that a comment is added to the record outlining their concerns.
- If this avenue is unsuccessful then they may pursue a complaint under the NHS Complaints procedure in an attempt to have the information corrected or erased.
- They may further complain to the Information Commissioner, who may rule that any erroneous information is rectified, blocked, erased or destroyed.

- If a patient believes that a medical opinion is incorrect this should be recorded in the records and the patients concerns outlined, however the opinion must remain in the records.

Confidential Waste

- It is the responsibility of all members of the practice to ensure that any material which contains patient, staff sensitive i.e. salary details or practice confidential information is disposed of safely and appropriately.

5. Practice Confidential information

- All personal staff information is regarded as confidential
- It is the responsibility of the Practice Management Team to produce salaries, practice accounts and to deal with any other confidential practice information without disclosure.
- It is the responsibility of the Practice Management Team to provide individual members of staff with protected time to discuss confidential issues and to provide help and assistance appropriately.
- It is the responsibility of the Practice Management Team to provide the same opportunity to the partners as necessary.
- It is the responsibility of the Practice Management Team to ensure this policy is adhered to and to take the appropriate steps to protect the practice and the patients in the event that confidentiality is breached.
- Staff must not access any record that they do not have a legitimate right to access i.e. family or friends. To do so, is a criminal offence

6. Disclosing Patient Information

If patient information is disclosed to another agency or body for purposes other than direct patient care then the consent of the patient is to be obtained, except in exceptional circumstances or it is a requirement of the law.

Disclosure to the Police

There maybe a requirement to disclose patient information without consent, this would usually be, for what would have been, a serious arrestable offence as defined by the Police and Criminal Evidence Act. (Although serious arrestable offences no longer exist, only arrestable offences, the GMC recommend that Practices continue to abide by the list) These offences are shown at Annex E.

Where ever possible though, the patients consent should be obtained before information is disclosed unless it would impede or hamper any investigations.

The Police have set documented procedures when requesting information without consent or a court order. The practice should ask the Police to conform to these, unless it is a matter of life or death.

Even though it may have been demonstrated that a serious offence has been committed the practice may request that a court order is obtained before they release any information.

If patient information is to be disclosed, then the reason why must be recorded. If the patient has not given their consent and/or has no knowledge that information has been disclosed about them then the reasoning must be recorded and placed in a clinician's sealed envelope.

A sealed envelope is defined by the NHS Information Standards Board as "Providing the means of enabling patients and clinicians to restrict certain parts of patient's health information from normal sharing or access"

Compliance with an Act of Parliament
If a request is made for personal information to comply with the law then the organisation that is requesting the information must state in writing under which Act of Parliament and which section of that Act they require the information, how much information they require and it must be requested by a person that is of sufficient seniority within there own organisation to accept responsibility for that organisation

Disclosure to the Courts
The courts, including coroner's courts have legal powers that require that information that may be relevant to matters within their jurisdiction be disclosed. This does not require the consent of the patient whose records are to be disclosed but he/she should be informed, preferably prior to disclosure.

Disclosures must be strictly in accordance with the terms of the order. If the order compels the practice to disclose what appears to you to be
irrelevant information, such as information about a patient's relative then such ethical concerns must be raised with the judge or presiding officer. If, however, the order is not amended, it must be complied with.

In the Public Interest
Only a court can ultimately decide what is or is not in the public interest. Any member of staff making a disclosure in the public interest will be expected to justify their reasoning, this could be to the courts or their regulatory body.

Disciplinary Action
If any member of staff fails to adhere to this guidance the practice may take such disciplinary action as it feels appropriate. This may include dismissal for serious breaches or referral to the appropriate regulatory body.

7. Associated Documents

NHS Confidentiality Code of Conduct -
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

GMC: Confidentiality Protecting and Providing Information –

http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp

BMA Confidentiality & Health Records

https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records

Information Commissioner's Office

www.ico.org.uk

Annex A

Data Protection Act 2018 Principles

1. Fairly, lawfully and transparently processed – inform people why you are collecting their information and what you are going to do with it.

2. Purpose Limitation– only use personal information for the purpose for which it was obtained, unless you have the persons consent to use it for another purpose, there is a legal requirement to disclose the information or disclosure can be justified as being in the public interest.

3. Data Minimisation - Adequate, relevant and not excessive – only collect and keep the information you require.

4. Accuracy - Accurate and kept up-to-date – Patients and staff should be regularly asked to verify the information the practice holds.

5. Storage Limitation – All records should be kept in accordance with NHS guidelines.

6. Integrity & Confidentiality - You must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Annex B

Rights of the individual

- A right to confirmation that their personal data is being processed and access to a copy of that data which in most cases will be Free of Charge and will be available within 1 month (which can be extended to two months in some circumstances)

- Who that data has or will be disclosed to;

- The period of time the data will be stored for – All Information be retained in accordance with the NHS Code of Practice for Records Management

- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;

- Data Portability – data provided electronically in a commonly used format

- The right to be forgotten and erasure of data does not apply to an individual's health record or for public health purposes

- The right to lodge a complaint with the Information Commissioner www.ico.org.uk

Annex C

Access to Health Records

Under the Data Protection Act any individual or their representatives with the consent of the individual has a right to receive a copy of their personal information that is held by the practice, usually their medical records The individual does not have to give any reason why they wish to see their records.

The most common reason for individuals requesting access to their records is for the purposes of minor compensations claims and the request will normally come from their solicitor.

Should a patient wish to see their records in situ they may do so, however the same rules apply as if they were receiving a copy of their records (as shown below). It may therefore not be practicable for the patient to view their original records.

Any request for access to records will, in the first instance, be dealt with by the Practice Manager and the following procedure should be followed.

1. A request may be made either verbally or in writing, including email. Where the request is in writing, it must be signed and dated by the individual. If at the time of receiving the request the authorisation is more than 6 months old a new authorisation from the individual is to be sought. This is to ensure that the individual still consents to the disclosure. If the request is made verbally, the individual must be known to the Practice. A record of the request must be kept

2. If there is any doubt as to the identity of the person, then evidence should be provided to prove their identity, such as their Council Tax Bill, anything from a Government Department, such as HMRC, Bank Statement or Utility Bill.

3. No fee will be charged for supplying a copy of the records, unless the request is deemed to be manifestly excessive or unfounded, for which we may charge a reasonable fee, which will include staff time. The practice regards more than two requests for the same record within one year of each other, as excessive.

4. For the purposes of clarity, if a request is received in June, that request will be free, if a subsequent request is received in January of the following year that will be free. If a further request is received in May, that will be regarded as a third request within a year and a fee maybe charged

5. If it is not clear what part of the record is to be accessed clarity should be sought from the individual or their representative.

6. The request must be complied with within one calendar month (30 days), An acknowledgement should be sent to the person making the request.

7. If it has been determined that a fee is to be charged, the requestor will be notified of the fee and the request will not be complied with until the fee has been received.

8. In the case of medical records, If access is requested to the whole record, good practice is that the patient is contacted to verify that they are happy for the release of the whole record. Many patients do not realise that if they authorise the full release of their records then matters such as their sexual health would also be released.

   The NHS Code of Confidentiality states "Ideally disclosure should be limited to the relevant incident concerned. However, if disclosure of the full record is required this should be complied with as long as it is clear that the patient understands that full disclosure will take place and has consented".

9. The appropriate records should be sourced and if they are manual (Lloyd George) records, they should be scanned into the clinical system. Any part of the record that contains third party information or information that may cause serious physical of mental harm the patient or another person, must be scanned in separately.

10. The appropriate health professional should then check the records before they are released and remove anything that they feel may cause serious physical or mental harm to either the patient or another person. The records should also be checked for any references to a third party or anything that may identify a third party (this can be done by anyone) and remove it, unless you have that person's explicit consent for it to remain in the record or the information about the third party provided by the patient or is already known to the patient, such as the name of a chaperone. All references to health professionals will remain.

11. If any part of the record is to be redacted, there is no obligation to mark where information has been removed nor is there a requirement to state that information has been redacted, when it would defeat the purpose of the redaction

12. If the records are to be sent out electronically then they must be encrypted to 256 AES. You should follow any guidance issued by the supplier of the encryption service

13. If the records are sent out in paper format, then as a minimum, they should be sent by recorded delivery.

14. The requestor cannot specify in what format they wish to receive the information, unless other legislation, such as disability legislation applies.

Access to a child's health record

For a person to have access to a child's health record that person must have parental rights. If it has been established that a child is Fraser / Gillick Competent consent must be obtained from the child before access is granted to either parent. If access is granted to a person with parental rights there is no requirement to inform any other person with parental rights that access to the records has been granted.

If access to a child's health record is granted to a person with parental responsibility, then any reference or action involving any other person, including another person with parental responsibility, which would identify them, must be removed unless you have that person's consent.

Where one parent is asking for access to a child's record, it may prove more practicable to be provided with the other parent's consent for the release of their information.

If the child has provided information in confidence, then this must not be released without the permission of the child

Parental rights are defined as:

Married Couples

Both of a child's legal parents have parental responsibility if they were married at the time of the child's conception or at some time thereafter If a child is legally adopted parental responsibility is transferred to the adopting family. In certain circumstances the Courts may grant parental responsibility to another person.

Unmarried Couples

For the father to have parental responsibility both parents must **register the birth of the child together**.

Divorced / Separated Couples

Parental responsibility remains with both parents even if they are divorced or have separated, unless the courts remove that responsibility.

The commonest reason for removing parental responsibility is because of neglect / abuse to a child by a parent(s)

If it is known that parents have divorced / separated and a parent is requesting access to the records the parent should clearly state that they still retain parental rights. They must provide the child's full name, date of birth and the address at which the child resides. This must match the information held by the practice

The records of the child should be checked to see if there are any entries that might indicate that parental rights could have been removed. If there are no such entries in the records it should be accepted that the parent still holds parental rights

If there are any entries in the records that might suggest that a parent has had parental rights removed the practice should seek further advice before the records are released.

Annex D

Access to records of the deceased

It is Department of Health and Social Care and General Medical Council policy that records relating to deceased people should be treated with the same level of confidentiality as those relating to living people. Access to the health records of a deceased person is governed by the Access to Health Records Act 1990. Under this legislation when a patient has died, their personal representative, executor or administrator or anyone having a claim resulting from the death (this could be a relative or another person), has the right to apply for access to the deceased's health records.

A request for access should be made in writing to ensure that it contains sufficient information to enable the correct records to be identified.

The request should also give details of the applicant's right to access the records, this should be where ever possible be by producing a copy of the deceased persons will.

If the deceased person had indicated that they did not wish information to be disclosed, or the record contains information that the deceased person would have expected to remain confidential then it must remain so.

In addition, the record holder has the right to deny or restrict access if it felt that disclosure would cause serious harm to the physical or mental health of any other person, or would identify a third person.

In line with GMC guidance family members may be informed of any information that directly relates to the cause of death. Unless the deceased person had indicated they did want the information released.

Annex E

Serious Arrestable Offences as defined by the Police and Criminal Evidence Act

- Treason
- Murder
- Manslaughter
- Rape
- Kidnapping
- Incest or intercourse with a girl under 13
- Buggery with a boy under 16
- Indecent assault constituting gross indecency
- Causing an explosion likely to endanger life or property
- Certain offences under the Firearms Act 1968
- Causing death by dangerous driving
- Hostage taking
- Torture
- Many drug-related offences
- Ship hijacking and Channel Tunnel train hijacking
- Taking indecent photographs of children
- Publication of obscene matter