The South London Private GP

Enhancing Life, Excelling in Care

Policy Number: IG03

Confidentiality & Data Protection Policy

Document name	Confidentiality & Data Protection Policy
Document Classification:	Information Governance
Document No:	IG03
Version:	1.0
Name of originator/author:	Dr Thomas Quinn
Policy Owner:	Caldicott Guardian
Date created	26/09/18
Date reviewed	
Date ratified:	
Ratified by:	Executive Board
Name of responsible committee:	Information Governance Steering Group
Superseded policy (if applicable):	
Next review date:	01/10/20
Target audience:	All staff
Date published to Intranet site:	

SUMMARY

Everyone working for THE SOUTH LONDON PRIVATE GP LTD. has a legal duty to keep information about patients confidential. THE SOUTH LONDON PRIVATE GP LTD. requires all staff who receive or have access to information regarding patients or staff, or information regarded as ‘commercial – in confidence’, to keep it confidential. The confidentiality of patient information is an essential component of Clinical Governance and Information Security.

The Caldicott Committee’s report on the Review of Patient-Identifiable Information was published in December 1997. The Committee made a number of recommendations aimed at improving the way Healthcare Providers handle and protect patient information. The requirement for organisations to appoint guardians of patient information (Caldicott Guardians) was a product of the Government’s commitment to implementing the recommendations of the Report. The Caldicott Guardian for THE SOUTH LONDON PRIVATE GP LTD. is an Executive Director .

Table Of Contents

1. INTRODUCTION AND POLICY PRINCIPLES 5
2. CONDITIONS OF EMPLOYMENT 6
3. DATA PROTECTION 7
4. SCOPE (Data Protection Act) 8
5. COMMERCIAL CONFIDENTIALITY 12
6. PATIENT INFORMATION AND OTHER AGENCIES 12
7. RELATIVES / NEXT OF KIN 12
8. VULNERABLE ADULTS 13
9. CHILDREN 13
10 STATUTORY REQUIREMENTS 14
11. RESEARCH, AUDIT AND MONITORING 14
12. PUBLIC INTEREST, POLICE AND LEGAL ENQUIRIES 14
13. MEDIA 15
14. HEALTH RECORDS (CASE NOTES) 15
15. ACCESS TO HEALTH RECORDS 16
16. VERBAL COMMUNICATION 18
17. BREACH OF CONFIDENCE 18
18. DISPOSAL OF CONFIDENTIAL PAPER WASTE 18
19. PATIENT CONFIDENTIALITY AND THE USE OF THE FAX MACHINE 18
20. Implementation Plan 19
21. REFERENCES 20
22. VERSION HISTORY TABLE 21
Appendix 1 22
Appendix 2 24

● 1. INTRODUCTION AND POLICY PRINCIPLES

Everyone working for THE SOUTH LONDON PRIVATE GP LTD. has a legal duty to keep information about patients confidential. OHL requires all staff who receive or have access to information regarding patients or staff, or information regarded as 'commercial – in confidence', to keep it confidential. The confidentiality of patient information is an essential component of Clinical Governance and Information Security.

The Caldicott Committee's report on the Review of Patient-Identifiable Information was published in December 1997. The Committee made a number of recommendations aimed at improving the way Healthcare Providers handle and protect patient information. The requirement for organisations to appoint guardians of patient information (Caldicott Guardians) was a product of the Government's commitment to implementing the recommendations of the Report. The Caldicott Guardian for THE SOUTH LONDON PRIVATE GP LTD. is an Executive Director.

The Caldicott Committee developed a set of general principles that, in essence, capture the directions of the Caldicott Report:

- Justify the purpose(s). Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined, scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

- Don't use patient-identifiable information unless it is absolutely necessary. Patient identifiable information items should not be used unless there is no alternative.

- Use the minimum necessary patient-identifiable information.

- Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

- Access to patient-identifiable information should be on a strict need to know basis. Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

- Everyone should be aware of their responsibilities.

- Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are aware of their responsibilities and obligations to respect patient confidentiality.

- Understand and comply with the law. Every use of patient-identifiable information must be lawful. In every organisation the Caldicott Guardian is responsible for overseeing arrangements to ensure that the organisation complies with legal requirements.

Patients should be assured that confidentiality will be maintained, and given examples of the permissible disclosure of information, such as for audit, research, data collection or teaching purposes. In these cases patients are not personally identified.

The term ‘case notes’ includes all written information concerning named patients, including medical records, nursing records and records made by other professionals, clerical and healthcare workers.

Care should be taken that the use of ‘aide memoirs’, file notes, notebooks, diaries and information written on ward and department ‘white boards’ or pinned on notice boards does not constitute or contribute to a breach of confidentiality.

Staff must be aware that the use of ‘global’ e-mails when seeking ‘mislaid’ notes may constitute a potential breach of confidentiality. Use the minimum information; surname, Reference number and contact rather than details of the patient’s attendance and restrict the circulation as much as possible.

Care must be taken to ensure that faxes, which contain essential patient-identifiable information, are sent only to the intended recipient (usually a GP or other healthcare agency). It is good practice to telephone in advance of such fax transmissions and to use a cover sheet advising that the information is confidential is intended only for the named individual and a telephone number to contact in case of the fax being received in error.

The same principles of confidentiality apply to:

- Personal / Human Resources records
- Occupational health department documentation
- Records of staff who attend THE SOUTH LONDON PRIVATE GP LTD. clinic’s as a patient

- **2. CONDITIONS OF EMPLOYMENT**

Conditions of Employment, issued as part of every employee’s contract states that **‘***whilst you are employed at* THE SOUTH LONDON PRIVATE GP LTD. *you will come into contact with confidential information / data relating to the work of* THE SOUTH LONDON PRIVATE GP LTD. *its patients or staff. You are bound by your conditions of service to respect the confidentiality of any information you may come into contact with which identifies patients, staff or other* THE SOUTH LONDON PRIVATE GP LTD. *personnel and / or the business information of* THE SOUTH LONDON PRIVATE GP LTD.*. Under no circumstances should*

such information be divulged or passed to any unauthorised persons or organisations. You could also face prosecution under the Data Protection Act 1998'.

Disciplinary action will be taken against an employee who is found to have breached confidentiality. They could also face prosecution under the Data Protection including General Data Protection Regulation (GDPR) 2018.

Media enquiries should be referred to the CEO without exception.

Where employees who use a computer misuse their rights of access to computer information, e.g. disclose their password to someone else or use someone else's password to gain access to databases, they could be disciplined which could lead to dismissal. They may also be prosecuted under the Computer Misuse Act 1990.

Managers must ensure that confidentiality is discussed on the first day of employment with all new employees, as part of an induction checklist. It is recommended that staff sign to acknowledge that they have taken note of the contents of this policy.

Volunteers and work experience students must also have their role in maintaining confidentiality made clear by the member of staff responsible for them and must be aware of and adhere to this policy.

- **3. DATA PROTECTION**

Personal information relating to clients and staff is kept and stored either on written documents (hard copies) or on computers (soft copies).

All such information is confidential and access is available only to authorised personnel and subject to the Data Protection including General Data Protection Regulation (GDPR) 2018.

There are Seven principles of GDPR:

1. **Lawful, fair and transparent processing** – This principle emphasizes transparency for all EU data subjects. When the data is collected, it must be clear as to why the data is being collected and what the data will be used for. Organizations also must be willing to provide details surrounding the data processing when requested by the data subject. For example, if a data subject asks who the data protection officer is at that organization or what data the organization has about them, that information needs to be available.
2. **Purpose limitation** – This principle means that you need to have a lawful and legitimate purpose for processing the information in the first place. Consider all the organizations who make you fill out a form with 20 fields, when all they would need

to sell you that gadget is your name, email, shipping address and maybe a phone number in case they need to get a hold of you. Simply put, this principle says that organizations shouldn't collect any piece of data that doesn't have a specific purpose, and those who do can be out of compliance.

3. **Data minimization** – This principle instructs you to ensure the data you are capturing is adequate, relevant and limited. In this day and age, businesses collect and compile every piece of data possible on you for various reasons, such as understanding customer buying behaviours and patterns or remarketing based on intelligent analytics. Based on this principle, organizations must be sure that they are only storing the minimum amount of data required for their purpose.

4. **Accurate and up-to-date processing** – This principle requires data controllers to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the organization must have a process and policies in place to address how they will maintain the data they are processing and storing. It may seem like a lot of work – you can expect it to be – but a conscious effort to maintain accurate customer and employee database will help prove compliance and hopefully also prove useful to the business.

5. **Limitation of storage in the form that permits identification** – This principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached. To ensure compliance, organizations must have control over the storage and movement of data. This includes implementing and enforcing data retention policies and not allowing data to be stored in multiple places. For example, prevent users from saving a copy of a customer list a local laptop or moving the data to an external device such as a USB. Having multiple, illegitimate copies of the same data in multiple locations is a compliance nightmare.

6. **Confidential and secure** – This principle protects the integrity and privacy of data by making sure its secure (which extends to IT systems, paper records and physical security). An organization that is collecting and processing the data is now solely responsible for implementing the appropriate security measures that are proportionate to the rights and risk of the individual data subjects. Negligence is no longer an excuse under GDPR, so organizations must spend an adequate about of resources protecting the data from those who are both negligent or malicious. To get compliant, evaluate how well you are enforcing security policies, utilizing dynamic access controls, verifying the identity of those accessing the data, protecting against malware/ransomware, etc.

7. **Accountability and liability** – This principle ensures that you are able to demonstrate compliance. Organizations must be able to demonstrate to the governing bodies that they have taken the necessary steps comparable to the risk their data subjects face. To ensure compliance, be sure that every step within the GDPR strategy is auditable and can be compiled as evidence quickly and efficiently. For example, GDPR requires organizations to respond to requests from data subject as to what data is being held on them and promptly remove that data, if desired. You would not only need to have a process in place to manage the

request, but it would need to have a full audit trail to prove that you took the proper actions.

There are a large number of offences and penalties for contravening the Act and these include unlimited fines for knowingly or recklessly breaking the Statute.

- **4. SCOPE (DATA PROTECTION ACT)**

THE SOUTH LONDON PRIVATE GP LTD. is registered under the Data Protection Act for information in the following categories:

Purpose 1: Accounts and Records

Data Subjects are: Suppliers
Business or other contacts
Data Classes are: Personal details
Financial Details
Goods or services provided
Sources & Disclosures (1984 Act). Recipients (1998 Act):
Data subjects themselves
Healthcare, social and welfare advisers or practitioners
Suppliers, providers of goods and services
Financial organisations and advisers
Central Government
Transfers: None outside the European Economic Area

Purpose 2: Health Administration and Services

Data Subjects are: Relatives, guardians and associates of the data subject
Data Classes are: Personal details
Family, lifestyle and social circumstances
Employment details
Goods or services provided
Racial or Ethnic Origin
Religious or other beliefs of a similar nature
Physical or Mental Health or Condition
Sexual life
Sources & Disclosures (1984 Act). Recipients (1998 Act):
Data subjects themselves
Healthcare, social and welfare advisers or practitioners
Relatives, guardians or other persons associated with the subject data
Suppliers, providers of goods and services
Business associates and other professional advisers

Central Government

Transfers: None outside the European Economic Area

Purpose 3: Staff Administration

Data Subjects are: Staff including volunteers, agents, temporary and casual workers

Relatives, guardians and associates of the data subject

Data Classes are: Personal details

Family, lifestyle and Social Circumstances

Education and training details

Employment details

Financial details

Racial or Ethnic origin

Religious or other beliefs of a similar nature

Trade Union Membership

Physical or Mental Health or Condition

Sources & Disclosures (1984 Act)

Recipients (1998 Act):

Data subjects themselves

Relatives, guardians or other persons associated with the data Subject

Current, past or prospective employers of the data subject

Education, training establishments and examining bodies

Suppliers, providers of goods and services

Financial organisations and advisers

Employment and recruitment agencies

Central Government

Transfers: None outside the European Economic Area

The registration under the GDPR is administered by 12 Point Care Ltd.

Definition of terms

ACCESSING: To obtain access to data with the purpose of interrogating or amending the details of a particular data subject. Keeping the documents on computer and accessing them by name of the sender/recipient is included. Any operation performed only for the purpose of preparing the text of documents is excluded.

DATA: 'Information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose'. Data may also be defined as the raw material from which the information is derived.

PERSONAL DATA: Data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinions about the individual but excluding any indication of the intentions of the data user in respect of that individual'**.**

DATA USER: An organisation or individual who controls the contents and use of a collection of personal data processed, or intended to be processed automatically.

DATA SUBJECT: 'An individual who is the subject of personal data'.

DATA PROCESSING: 'Amending, augmenting, deleting or re-arranging the data or extracting the information constituting the data by reference to the data subject'

Staff compliance

For reasons of security and in order to restrict assess to personal data all staff observe the following:

I. Guidance of how to use the computer system (e.g. manuals) is not left on display.

II. Display Screen Equipment (DSE) is sited so that information cannot be seen by unauthorised persons.

III. DSE's are never left unattended whilst in use.

IV. Personal passwords are not displayed or relayed to other members of staff.

V. After using the DSE the operator logs off.

VI. Regular back ups of the system data and files are made.

VII. All disks are kept in a locked place separate from the master disks.

VIII. Access to the locked cabinets containing Personnel files is restricted to the HR Manager and Office Manager.

IX. Individual Personnel files can be viewed by the relevant Department Manager.

Confidentiality

All information relating to service users, **INCLUDING THEIR VERY PRESENCE IN THE SOUTH LONDON PRIVATE GP LTD. PREMISES** is regarded as confidential.

Any requests for information by the media are referred to the Office Manager.

Computer input and output paperwork is covered by the Act and care is taken to ensure that this is not left unattended.

To limit disclosure of personal data, all stationery posted to clients is posted in sealed envelopes. Window envelopes are used with only the service users name and address showing.

Unwanted paperwork is shredded or destroyed in a confidential waste disposal manner.

Real data is not used for training or demonstration purposes.

Personal Identifiable Information is stored on the computer system as an Electronic Patient Record and hard copy medical data is stored in individual patient folders within the Medical Records Store. Access to the computer system is restricted by the use of log-on codes and passwords.

Client Access

All individual clients and companies have the right to request personal data held by THE SOUTH LONDON PRIVATE GP LTD.

Fees

THE SOUTH LONDON PRIVATE GP LTD. will no longer be able to charge an individual for the administrative costs of finding, gathering and disclosing data to the individual unless the individual's request is "manifestly unfounded or excessive".

An example of a scenario where a fee could be charged is if a request is repetitive or if additional copies of the data are requested.

However, if the Subject Access Request is either unfounded, excessive or repetitive an THE SOUTH LONDON PRIVATE GP LTD. charge for dealing with the request by levying a "reasonable fee", to take into account the administrative costs of providing the information.

Timing

Under the Data protection Action, organisations had a deadline of 40 days to respond to a Data Subject Access Request. Post 25th May 2018 and under GDPR rules, information must be provided to the individual without delay, and at the latest, within one month of receipt of the request.

THE SOUTH LONDON PRIVATE GP LTD. can extend the deadline by a further two months where the individual's requests are complex or numerous. If this is the case, THE

SOUTH LONDON PRIVATE GP LTD. will notify the individual of this within a month of receipt of the request, providing its reasons for the delay.

Unfounded and excessive requests

In addition to being able to charge if the request is unfounded and/or excessive (for example if there is repetition in the request), THE SOUTH LONDON PRIVATE GP LTD. have a legal right to refuse to respond to the request.

If this is the case reasons for the refusal will be given to the individual. The individual must also be informed of their right to complain the Information Commissioners Office, and of their right to a judicial remedy.

Both the reasons for refusal and the advising of the right to complain must be put to the individual without undue delay and, at the very latest, within one month of the request.

If THE SOUTH LONDON PRIVATE GP LTD. processes a vast quantity of information about an individual, THE SOUTH LONDON PRIVATE GP LTD. may ask that individual to clarify what particular information they are referring to in the request. THE SOUTH LONDON PRIVATE GP LTD. will then be able to consider whether the scale of the information requested is 'unfounded' and/or 'excessive' and react to the request accordingly.

● 5. COMMERCIAL CONFIDENTIALITY

Many staff have access to commercial information, for example the cost of equipment or discounts which apply to THE SOUTH LONDON PRIVATE GP LTD.. This information must be treated as confidential, and only discussed / disclosed where this forms part of the employee's remit within the organisation.

● 6. PATIENT INFORMATION AND OTHER AGENCIES

Protocols governing the receipt and disclosure of patient information are clearly set out in the NHS Executive document 'Protecting and Using Patient Information – A Manual for Caldicott Guardians'. Details of this framework are provided in Appendix 1. 12 Point Care accepts the recommended framework and the need to develop clear protocols to support the practical implementation of this Confidentiality Policy.

Service users should be made aware of what happens to information about themselves. The Protection and Use of Patient Information – Guidance from the Department of Health, Annex A: Model Notice for Patients is adopted for use within THE SOUTH LONDON PRIVATE GP LTD. Treatment centres and offices and is included as Appendix 2.

Recommended methods of providing this information to patients include:

* Service users are informed via the Service user guide of their right to access medical records

* Routinely providing Service users with appropriate information as a part of care planning.
* Identifying someone able to provide more detailed information as required.

● 7. RELATIVES / NEXT OF KIN

The Patient's Charter says that *'if you agree, you can expect your relatives and friends to be kept up to date with the progress of your treatment*'. Such agreement needs to be explicitly secured, as the Human Rights Act 1998 (in force from October 2000) will open the way for legal challenge if specific, personal information is shared or disclosed without the patient's consent. Clinical staff must exercise caution when discussing a patient's condition with relatives or next of kin.

There may be occasions where, in the judgement of the managing clinician (but incorporating the advice of the wider multidisciplinary team as appropriate), knowledge of a patient's condition might seriously affect their physical or psychological well being if divulged to them. In these instances it may be decided to have discussions with the carer or next of kin. However a careful judgement will need to be made in view of the implications of the Human Rights Act, and the basis for the decision and the content of the discussion must be carefully documented.

In the event that a patient is not '*compos mentis*' and it is in the managing clinician's opinion that it is 'in the patient's best interest' that information be divulged to the carer or next of kin, this should take place with the recipient's understanding that it is given in confidence.

The patient's consent and recipient's understanding, date, time and place of interview, and those present should be documented in the patient's notes.

● 8. VULNERABLE ADULTS

Disclosure of abuse may be made by a vulnerable adult who may ask for that information to remain confidential and for no action to be taken. Staff should explain to the vulnerable adult or to their relative or carer, or anyone else seeking to disclose concerns about abuse, that they may not be able to keep all information confidential.

Staff have a duty to alert their line manager, or a more senior manager if they are made aware of any actual or potential abuse of patients. Failure to do so will lead to disciplinary action. This is important for the protection of the person reporting the abuse, and also for the safety and protection of other potential victims of the abuser's behaviour.

Staff must not disclose information to any third party, as a decision about who needs to be told will be made by a senior manager.

All agencies receiving information in the course of an investigation must treat it as confidential, although priority must at all times be given to the protection of the vulnerable person. Other agencies must not disclose information for any purpose without the consent of the professional or senior manager who provided it. The person at risk should be advised when information is passed to other professionals or key individuals.

● 9. CHILDREN

Special conditions apply to children as patients of THE SOUTH LONDON PRIVATE GP LTD.. (See Protection and Use of Patient Information – Guidance from the Department of Health section 4.10 and 4.11)

Children under the age of 16 who have the capacity and understanding to take decisions about treatment are entitled to decide whether personal information may be passed on and to have their confidence respected. In other cases, decisions to pass on personal information may be taken by a person with parental responsibility in consultation with the health professionals involved. (Young people aged 16 and over are treated as adults in respect of the law.)

In child protection cases the overriding principle is to secure the best interests of the child. Therefore, if a health professional or other member of staff has knowledge of abuse or neglect it may be necessary to share this with others on a strictly controlled basis so that decisions relating to the child's welfare can be taken in the light of all relevant information. In the first instance, the member of staff should seek advice from their line manager.

● 10 STATUTORY REQUIREMENTS

There are some instances where there is a statutory responsibility to pass on information. Prior consultation with the patient is not required but may be judged appropriate. If there are any doubts legal advice should be sought. The patient and relevant health professional should be informed as soon as possible and a note made in the patient's record. Statutory notification is required for:

- Births and deaths
- Communicable diseases
- Abortion
- Substance misuse
- Serious incidents – see Serious Untoward Incident Policy
- Certain obligations under the Mental Health Act 1983 and Mental Capacity act 2005

It is the responsibility of named officers of the organisation to pass on this information to the relevant body.

● 11. RESEARCH, AUDIT AND MONITORING

Access to patient identifiable information or anonymous data may be sought for research, audit or monitoring purposes, either by THE SOUTH LONDON PRIVATE GP LTD. employees or by other individuals or organisations.

Internal requests related to research projects must be approved by the CMO following discussion with the Relevant Ethics Committee and a formal submission will be required.

● 12. PUBLIC INTEREST, POLICE AND LEGAL ENQUIRIES

There may be a conflict between an employee's role as a Health Professional and as a 'responsible citizen'. Consideration will need to be given to the 'best interests' not only of the patient but also of other individuals or society in general. Some guidance is provided for registered healthcare professionals in their respective Codes of Conduct, but advice may also be sought directly from the professional's registering body, Professional Organisation or Trade Union.

The Police do not have automatic rights to information about a patient's personal or medical information. The matter should always be referred to the Office Manager unless there is immediate threat to human life as a result of the patient's actions.

A formally issued Court Order directed by a Judge or other presiding Officer is required in order to release information for legal proceedings. Verbal or written requests from lawyers are not sufficient. This type of request must be referred to the Office Manager who will seek advice from the Company Legal Dept.

● 13. MEDIA

All media enquiries must be directed to the CEO without exception.

● 14. HEALTH RECORDS (CASE NOTES)

Staff must ensure that medical case notes and nursing and other professional records are:

- Kept in secure locations at all times
- Secure when being transported throughout the Organisation
- Not left unattended in public areas.
- Tracked to locations to which they are forwarded.
- Not removed from THE SOUTH LONDON PRIVATE GP LTD. offices premises

- Offices and departments containing records must be kept locked when staff are absent.

Transportation of case notes:

Movement of case notes from the by THE SOUTH LONDON PRIVATE GP LTD. is carried out by THE SOUTH LONDON PRIVATE GP LTD.'s designated driver. Patients should not normally be asked to take responsibility for transferring their notes between sites.

There may be some instances when copies are made and sent with the patient in a sealed envelope.

NB It is not acceptable for clinicians to leave case notes unattended in a private vehicle

● 15. ACCESS TO HEALTH RECORDS

A Health Professional may allow patients access to their own particular section of clinical records, but they are NOT at liberty to disclose any other details relating to the clinical records of other Health Professionals.

This informal access is not regarded as access under the Act. Alternatively a patient can formally request access, should informal access be denied under the Act, by making a formal application to the 'holder' of these records.

The 'holder' of the record is defined as being:

- The patient's General Practitioner of Family Health Services Authority
- The Health Service body by which, or on whose behalf of, the record is held.
- The Health Professional by whom, or on whose behalf of, the record is held.

Who can apply for the Right of Access:

I. The patient (service user)
II. A personal representative of a deceased patient, or a person having a claim arising from the death.
III. A person authorised in writing to apply on behalf of the patient.
IV. A person having parental responsibility for a child under 16 years of age.
V. A person appointed by the Court to manage the affairs of a patient who is deemed incapable.

The holder of the record must be satisfied that the patient (or other authorised person) is capable of understanding the nature of the application before Access is given.

Cases where access may be *wholly* excluded:

I. If the patient (service user) has not consented to the application.
II. If the records of a deceased patient include a notes made at the patient's request that access, after death, was not to be granted.

III. If the application is made by a child under the age of 16 years, unless the holder is satisfied that the child is capable of understanding the nature of the application.

Cases where access may be *partially* excluded:

I. Where access would disclose information provided by an individual other than the patient, which would identify that individual, unless that individual consents, or is a Health Professional involved in the care of the patient.

II. Where, in the opinion of the holder, access is likely to cause serious harm to the mental or physical health of the patient or any other individual.

III. Where the expectation of the patient was that any information was not to be disclosed.

IV. Where, in the opinion of the holder, an application is made by an individual having a claim arising from the patient's death and the requested information is not relevant.

V. The Health Professional may use their discretion to decide if information recorded prior to November 1991 will help understanding and should, therefore, be disclosed.

Following a formal application, and when agreement has been obtained from the holder as to the entitlement, the applicant may inspect the record and take a copy of the record or an extract. Any terms used which are not intelligible to a layman must be explained.

If the holder receives an application with insufficient information to identify the record, further information must be requested within 14 days.

Corrections:

If a person considers any part of the information to be inaccurate, an application can be made in writing for the necessary correction. If the holder is satisfied that the information is incorrect, the alteration can be made. If the holder is not satisfied, then a note must be made of the information thought to be inaccurate and a copy of either correction or note given to the applicant.

If clinicians, of any discipline, who have entered details in manual records wish to share this information with their patients, this is permissible.

Patients and their relatives must not be handed their medical records for perusal unless a healthcare professional is available to:

- Be able to answer questions related to the contents of the medical record.
- Ensure that sections of the record are not removed.

Members of staff who receive requests for disclosure of medical records and are in any doubt about how to proceed should refer to the **IG Manager**.

● 16. VERBAL COMMUNICATION

Staff employed by THE SOUTH LONDON PRIVATE GP LTD. have a duty to ensure that patient information is divulged only in accordance with the patient's wishes.

Care should be taken when talking to patients or relatives that the conversation is not overheard inappropriately. Private facilities should be offered for interviews of a sensitive nature.
Staff should satisfy themselves that information regarding a patient's condition or diagnosis over the telephone is only given within the principles of these guidelines and that the identity of the caller is correctly established. Care should also be taken as to who may overhear telephone conversations.

● 17. BREACH OF CONFIDENCE

Any instance of unauthorised passing on of patient information may result in disciplinary action.

Patients who feel that confidentiality has been breached may wish to use the complaints procedure. Patients have a right to be given advice about the complaints procedure.

● 18. DISPOSAL OF CONFIDENTIAL PAPER WASTE

Confidential paper waste bins are situated in every office throughout the organisation.

When the confidential bags are full, they will be collected them and ensure confidential disposal

Once sacks of waste have been disposed THE SOUTH LONDON PRIVATE GP LTD. is issued with a certificate of disposal.

The Certificates are filed at Head Office, this is a sub contracted service.

● 19. PATIENT CONFIDENTIALITY AND THE USE OF THE FAX MACHINE

The fax machine in the business office is the designated "safe-haven" fax machine

The office is kept locked when not in use to ensure the fax machine is not left unattended

The key to the business office is only issued to authorised staff

The fax cover sheet is always used which carries a warning if there was an error in transmission (Form [##])

- **20. Implementation Plan**

Consultation
Stakeholders and sub-contractors will be made aware of this policy and offered the opportunity to comment or advise on content. Patient forum will asked for comments.

Ratification
Board ratification has been sought for this policy

Dissemination
The policy will be made available to all staff on THE SOUTH LONDON PRIVATE GP LTD. Shared drive

Training/Awareness
The policy will be introduced to all staff at induction and reviewed at annual appraisal or supervisory session.

Audit and/or Monitoring
This policy will be monitored, assessed and reviewed through incident reporting and supervisory sessions. The IGSG is responsible for review and the frequency that this review will be carried out.

Compliance with this policy will be monitored through the ratification process and overseen by the IGSG.

It will be the day to day responsibility of all managers to monitor that the requirements of this procedure are being adhered too, and that appropriate risk control measures are in place.

Managers are responsible for ensuring effected staff have followed the reporting and management procedures highlighted in this policy.

Adverse event reporting will also be used to ensure compliance with procedures.

Breach of this Policy

This policy is mandatory and all staff must implement this policy and follow the procedures associated with it. Non-compliance with the policy and procedures will be dealt with in accordance with agreed disciplinary procedures.

● 21. REFERENCES

GDPR 2018.
Confidentiality, section 3.9 Access to Health records. NHSE 1996.
HSC 1998/089 Implementing the Recommendations of the Caldicott Report. NHSE, 1998.HSC HSG (96) 18. The Protection and Use of Patient Information. DOH, 1996.
Human Rights Act 1998.
Protecting and Using Patient Information – A Manual for Caldicott Guardians. NHSE, 1999.
Mental Capacity Act 2005

22. VERSION HISTORY TABLE

VERSION	DATE UPDATED	UPDATED BY	REASONS

-

● APPENDIX 1

CALDICOTT COMMITTEE – FRAMEWORK FOR THE SHARING OF PERSONAL INFORMATION

1. Outline

1.1 This framework document contains six sections:

- Objectives of a locally agreed protocol
- General principles governing the sharing of personal information
- Setting parameters for sharing personal information
- Defining purposes for which personal information is required
- Holding personal information, access and security
- Ownership of information and the rights of individuals

2. Objectives

2.1 To set parameters for the sharing of information between agencies which contribute to the health or social care of an individual.

2.2 To define the purposes for holding personal information within each agency.

2.3 To define how personal information should be held within each agency and who should have access to this information.

2.4 To define which information is designated as health services information and which is designated as social services information and to specify the rights of access to each for individuals as required by legislation.

3. General principles

3.1 Whilst it is vital for the proper care of individuals that those concerned with that care have ready access to the information that they need, it is also important that service users and their careers can trust that personal information will be kept confidential and that their privacy is respected.

3.2 All staff have an obligation to safeguard the confidentiality of personal information. This is governed by law, their contracts of employment, and in many cases by professional codes of conduct. All staff should be made aware that breach of confidentiality could be a matter for disciplinary action and provides grounds for complaint against them.

3.3 Although it is neither practicable nor necessary to seek an individual's specific consent each time that information needs to be passed on for a particular purpose that has been defined within this protocol, this is contingent on individuals having been fully informed of the uses to which information about them may be put. All agencies concerned with the care of individuals should satisfy themselves that this requirement is met.

3.4 Clarity about the purposes to which personal information is to be put is essential, and only the minimum identifiable information necessary to satisfy that purpose should be made available. Access to personal information should be on a strict need to know basis.

3.5 If an individual wants information about themselves to be withheld from someone, or some agency, which might otherwise have received it, the individual's wishes should be respected unless there are exceptional circumstances. Every effort should be made to explain to the individual the consequences for care and planning, but the final decision should rest with the individual.

3.6 The exceptional circumstances which override an individual's wishes arise when the information is required by statute or court order, where there is a serious public health risk or risk of harm to other individuals, or for the prevention, detection or prosecution of serious crime. The decision to release information in these circumstances, where judgment is required, should be made by a nominated senior professional within the agency, and it may be necessary to take legal or other specialist advice.

3.7 There are also some statutory restrictions on the disclosure of information relating to HIV and AIDS, other sexually transmitted diseases, assisted conception and abortion.

3.8 Where information on individuals has been aggregated or anonymised, it should still only be used for justified purposes, but is not governed by this protocol. Care should be taken to ensure that individuals cannot be identified from this type of information, as it is frequently possible to identify individuals from limited data e.g. age and post code may be sufficient.

4. Setting parameters

4.1 There should be a nominated senior professional, within each agency covered by this protocol, responsible for agreeing amendments to the protocol, monitoring its operation, and ensuring compliance.

4.2 Personal information should be transferred freely between the agencies who have agreed and are complying with this protocol, for the purposes it defines. A regularly updated register of individuals who need access to personal information, and the defined purpose for which they need this access, shall be made available to each agency concerned.

4.3 If appropriate, service level agreements can be used to establish standards for sharing information, e.g. speed of response.

4.4 Specific consent is required prior to personal information being transferred for purposes other than those defined in this protocol, unless there are exceptional circumstances as outlined above.

4.5 Where individuals are unable to give consent, the decision should be made on the individual's behalf by those responsible for providing care, taking into account the views of patients and careers, with the individual's best interests being paramount. Where practicable, advice should be sought from the nominated senior professional and the reasons for the final decision should be clearly recorded.

5. Defining purposes

5.1 There will be a range of justifiable purposes to be locally agreed. The following list is not exhaustive

- delivering personal care and treatment
- assuring and improving the quality of care and treatment
- monitoring and protecting public health
- managing and planning services
- risk management
- investigating complaints and notified or potential legal claims
- teaching
- statistical analysis
- medical or health services research

6. Holding information, access and security

6.1 Staff should only have access to personal information on a need-to-know basis, in order to perform their duties in connection with one or more of the purposes defined above. Clinical and professional details should be available to all those, but only those, involved in the care of the individual.

6.2 Each agency will ensure that they have mechanisms in place to enable them to address the issues of physical security, security awareness and training, security management, systems development, site specific information systems security policies, and systems specific security policies.

6.3 Each agency will take all reasonable care and safeguards to protect both the physical security of information technology and the data contained within it.

6.4 All information systems will be effectively password protected and users will not divulge their password nor leave systems active whilst absent.

6.5 All personal files and confidential information must be kept in secure, environmentally controlled locations when unattended, e.g. in locked storage cabinets, security protected computer systems etc.

6.6 Keys to lockable storage cabinets should be held only be staff who require regular access to the information they contain. Keys must be held in a secure place.

7. Ownership of information and the rights of individuals

7.1 Whilst written and computerized records will be regarded as shared between the agencies, an individual's right of access to the information contained in the records differs when it has been provided by a health professional from when it has been provided by Social Services staff.

7.2 Any health professional contribution to records maintained by Social Services staff, whether a letter, a case record or a report, must be clearly marked as such, and where practicable, kept in a closed part of the file. Social Services staff cannot grant access to this information without written authorization.

7.3 The reverse also applies. Staff cannot grant access to Social Services information without written authorisation.

● APPENDIX 2

PROTECTION AND USE OF PATIENT INFORMATION – NOTICE FOR PATIENTS

We *ask* you for information so that you can receive proper care and treatment.
We *keep* this information, together with details of your care, because it may be needed if we see you again.
We *may use* some of this information for other reasons: for example, to help us protect the health of the public generally and to see that THE SOUTH LONDON PRIVATE GP LTD. runs efficiently, plans for the future, trains its staff, pays its bills and can account for its actions. Information may also be needed to help educate tomorrow's clinical staff and to carry out medical and other health research for the benefit of everyone.
Sometimes the law requires us to *pass on* information: for example, to notify a birth.
You have a right of access to your health records.

Everyone working for THE SOUTH LONDON PRIVATE GP LTD. has a legal duty to keep information about you confidential.
You may be receiving care from other people as well as THE SOUTH LONDON PRIVATE GP LTD.. So that we can all work together for your benefit we may need to share some information about you. We only ever use or pass on information about you if people have a genuine need for it in your and everyone's interests. Whenever we can we shall remove details which identify you.
Anyone who receives information from us is also under a legal duty to keep it confidential.
If you agree, your relatives, friends and carers will be kept up to date with the progress of your treatment.

The main reasons for which your information may be needed are:

- giving you health care and treatment
- looking after the health of the general public
- managing and planning ,for example:
    - (where steps will be taken to ensure you cannot be identified) making sure that our services can meet patient needs in the future
    - paying your doctor, nurse, dentist, or other staff, and the treatment centre which treats you for the care they provide
    - auditing accounts
    - preparing statistics on performance and activity
    - investigating complaints or legal claims
- helping staff to review the care they provide to make sure it is of the highest standard
- training and educating staff (but you can choose whether or not to be involved personally)

If at anytime you would like to know more about how we use your information you can speak to the person in charge of your care.