GDoc Limited

Confidentiality Policy

Last revised	June 2018
Last reviewed	June 2018
Owner	JB

Adapted from the NHS England Confidentiality Policy June 2016, Document Number: POL_1010

1. Introduction

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within GDoc's services and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 1998. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

It is important that GDoc protects and safeguards person- identifiable and confidential business information that it gathers, creates processes and discloses, in order to comply with the law, relevant NHS mandatory requirements and to provide assurance to patients and the public.

This policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non NHS organisations.

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted as per current NHS Encryption Guidance or a business case has been approved by the Transformation & Corporate Operations Directorate Information Governance TeamConfidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc. It also includes GDoc confidential business information.

Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.A summary of Confidentiality Do's and Don'ts can be found at Appendix A.

The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles of this policy can be found in Appendix B.

How to report a breach of this policy and what should be reported can be found in Appendix C.

Definitions of confidential information can be found in Appendix D.

Roles and Responsibilities

The Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that GDoc policies comply with all legal, statutory and good practice guidance requirements.

The Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient-identifiable information.

All staff

Confidentiality is an obligation for all staff. Staff should note that they are bound by the Confidentiality: NHS Code of Practice 2003. There is a Confidentiality clause in their contract and that they are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

Any breach of confidentiality, inappropriate use of health, staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract,and must be reported.

Corporate Level Procedures

Principles

All staff must ensure that the following principles are followed:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.

- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with your Line Manager or the Clinical Lead.

GDoc is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

1. Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.
2. Access to rooms and offices where terminals are present or person-identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.
3. All staff should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.
4. Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

<u>Disclosing Personal/Confidential Information</u>

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

If staff are unsure whether information can be disclosed, they must check with their line manger (or, in his/her absence, a senior member of staff), before disclosure.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing/Information Sharing, Data Re-

Use or Data Transfer Agreement will have been completed before any information is transferred.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail. See the Safe Haven Procedure for guidance on the safe transfer of confidential or person-identifiable information.

Transferring patient information by email to anyone outside the NHS may only be undertaken by using encryption as per the current NHS Encryption Guidance or through an exchange within the NHS Mail system (i.e. from one NHS.net account to another NHS.net account or to a secure government domain e.g. gsi.gov.uk), since this ensures that mandatory government standards on encryption are met. Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person-identifiable or confidential information.

Working Away from the Office Environment

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

Taking home/ removing paper documents that contain person-identifiable or confidential information from GDoc premises is discouraged.

To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

When working away from GDoc locations staff must ensure that their working practice complies with GDOc's policies and procedures. Any electronic removable media must be encrypted as per the current NHS Encryption Guidance.

Staff must minimise the amount of person-identifiable information that is taken away from GDoc premises.

If staff do need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of GDoc's buildings.
- Confidential information is kept out of sight whilst being transported.

If staff do need to take person-identifiable or confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not store person- identifiable or confidential information on a privately-owned computer or device.

Staff may use privately owned computers and other devices to access GDoc-related email, provided that the device is linked to a private, password-protected Wifi network.

If using a privately-owned device to access email, staff must ensure that they do not store person-identifiable or confidential information on it, even inadvertently. Any documents downloaded must be closed, deleted and the Trash/Recycle folder cleared at the end of each session.

If staff feel that there is a need to use a privately-owned computer or device to work more extensively than simply accessing email (for example if they choose to contribute to a work project while on leave), this must be agreed by their line manager in advance. The line manager will undertake a risk assessment, to include the nature of the data to be accessed and the security arrangements, which should include access to a secure Wifi network, a complex password and, wherever possible, the facility to erase the data remotely, in the case of the device being lost or stolen. At the end of each work session, any documents with person-identifiable or confidential information should be emailed to the member of staff's NHS.net email for storage, and the original deleted from the device, with the Trash/Recycle folder then being cleared.

Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally.

Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents, and
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended

Steps must be taken to ensure physical safety and security of person- identifiable or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal.

Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by GDoc' policies and procedures.

If staff have concerns about this issue they should discuss it with their Line Manager or the Clinical Lead.

Appendix A: Confidentiality Dos and Don'ts Dos

Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of GDoc.

Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.

Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.

Do ensure that you cannot be overheard when discussing confidential matters.

Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.

Do share only the minimum information necessary.

Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk.

Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent, and record the decision and any action taken.

Do report any actual or suspected breaches of confidentiality.

Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don't share passwords or leave them lying around for others to see.

Don’t share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.

Don’t use person-identifiable information unless absolutely necessary, anonymise the information where possible.

Don’t collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B: Summary of Legal and NHS Mandated Frameworks

GDoc is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of GDoc, who may be held personally accountable for any breaches of information security for which they may be held responsible. GDoc shall comply with the following legislation and guidance as appropriate:

The Data Protection Act (1998) regulates the use of “personal data” and sets out eight principles to ensure that personal data is:

1. Processed fairly and lawfully.
2. Processed for specified and lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and where necessary kept up to date.
5. Not kept longer than necessary, for the purpose(s) it is used.
6. Processed in accordance with the rights of the data subject under the Act.
7. Appropriate technical and organisational measures are be taken to guard against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data
8. Not transferred to countries outside the European Economic Area (EEA) without an adequate level protection in place.

The Caldicott Report (1997) and subsequent Caldicott or National Data Guardian reviews) recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information.
- Don’t use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law.

The duty to share information can be as important as the duty to protect patient confidentiality

https://www.gov.uk/government/publications/the-information-governance-review

https://www.gov.uk/government/publications/caldicott-information-governance-review-department-of-health-response

Article 8 of the Human Rights Act (1998) refers to an individual's "right to respect for their private and family life, for their home and for their correspondence". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The Computer Misuse Act (1990) makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
3. Unauthorised acts with the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

and Making, supplying or obtaining articles for use in offences 1-3

The NHS Confidentiality Code of Practice (2003) outlines for main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law

Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is "ultra vires", i.e. beyond its lawful powers.

The NHS Care Record Guarantee

The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients' rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:

- Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:
    - You ask us to do so.
    - We ask and you give us specific permission.
    - We have to do this by law.
    - We have special permission for health or research purposes; or
    - We have special permission because the public good is thought to be of greater importance than your confidentiality, and
    - If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of Practice and other national guidelines on best practice.
- Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.

Appendix C: Reporting of Policy Breaches **What should be reported?**

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported to your line manager. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager or the Clinical Lead. The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to GDoc systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and NHS Code of Confidentiality.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing off person- identifiable information in ordinary waste paper bin.

<u>Seeking Guidance</u>

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or the Clinical Lead should be sought.

Reporting of Breaches

Any breaches of confidentiality of person-identifiable or confidential information shall be treated as a Significant Event and reported and analysed accordingly, with learning shared. The information will enable the monitoring of compliance and improvements to be made to the policy and procedures.

Appendix D: Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-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 etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive/confidential personal information as defined by the Data Protection Act 1998 refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.