Confidentiality Policy

Inmind Reference:	GDPR04
Category:	Governance/GDPR Policies
Version Number:	V2.0
Reviewed on:	February 2019
Next review date:	February 2020
Lead Officer:	Director of Contracts
Equality Impact Assessment completed:	Yes

Applicable Legislation/Regulations:
Human Rights Act 1998 Data Protection Act 1998 Data Protection Act 2018 Common Law Duty of Confidentiality Freedom of Information Act 2000 Access to Health Records Act 1990 Public Interest Disclosure Act 1998 Information Security Standards – ISO/IEC 17799: 2005 and IS Management NHS Code of Practice General Data Protection Regulation 2018
Codes of Practice:
The Caldicott Report 1997 and '7' Guidelines The NHS Confidentiality Code of Practice Policy Statement on Information Security and Governance
Purpose:
To ensure that Inmind Healthcare has in place a comprehensive Information Governance Framework to manage the processes for acquisition, processing, storage, sharing and disposing of the information assets for which it is responsible.

Version Control Table		
Date Ratified	**Version Number**	**Status**
September 2016	1.0	Closed
February 2020	2.0	Live

Date	**Key Revision**
February 2020	Ratified and put onto new policy template

Please check to ensure this is the most current electronic copy of this document as it is updated and published in electronic format only (hard copies may become out of date).

Equality Impact Assessment for this policy

Protected Characteristic (domain)	Area of conflict	Resolution
Age	Nil	N/A
Disability	Nil	N/A
Gender Reassignment	Nil	N/A
Pregnancy & Maternity	Nil	N/A
Race	Nil	N/A
Religion or Belief	Nil	N/A
Sex	Nil	N/A
Sexual Orientation	Nil	N/A
Marriage and Civil Partnership	Nil	N/A

All relevant persons are required to comply with this policy and must demonstrate sensitivity and competence in relation to diversity in race, faith, age, gender, disability and sexual orientation. If you feel you are disadvantaged by this policy, please contact the Registered Manager and the service will actively respond to the enquiry.

Contents

1. Statement

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within Inmind Healthcare Group 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. Along with a full understanding of the process in reporting a breach.

This policy aims to give guidance, if in doubt, seek advice from your line manager.

2. Introduction

2.1 All employees working at Inmind Healthcare Group are bound by a legal duty of confidence to protect personal information they may encounter during the course of their work. This is not just a requirement of their contractual responsibilities, this is also a requirement within the common law duty of confidence and the Data Protection Act 1998.

2.2 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 or sent via a secure NHS Net account in accordance with NHS Net Accounts Acceptable Use Policy – See Appendix A.

2.3 It is important that Inmind Healthcare Group protects and safeguards person identifiable and confidential business information that it gathers, creates processes and discloses, to comply with the law.

2.4 This policy sets out the requirements placed on all staff when sharing information within Inmind Healthcare Group and between other Inmind Healthcare Group hospitals and non Inmind Healthcare Group organisations.

2.5 A summary of Confidentiality Do's and Don'ts can be found at Appendix B.

3 Scope

All Staff working in or on behalf of Inmind Healthcare Group (this includes contractors, temporary staff, and all permanent employees).

4 Roles and Responsibilities

4.1 The Chief Executive.

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

4.2 The Caldicott Guardians.

4.2.1 The Caldicott Guardians are responsible for ensuring implementation of the Caldicott Principles with respect to patient-identifiable information. The principles are listed below:

- Principle 1 - Justify the purpose(s) for using confidential information
- Principle 2 - Don't use personal confidential data unless it is absolutely necessary
- Principle 3 - Use the minimum necessary personal confidential data
- Principle 4 - Access to personal confidential data should be on a strict need-to-know basis
- Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities
- Principle 6 - Comply with the law
- Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

4.3 Human Resources

4.3.1 Hospital Directors are responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in inductions for all staff, including access to HR records and confidential information.

4.3.2 Inmind Healthcare Group complies fully with the DBS Code of practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

4.3.3 Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

4.4 Senior Managers

4.4.1 Senior Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon. Although it is everyone's responsibility to report any breach to the Caldicott guardian Carmen Howarth-Tyler.

4.5 All staff

4.5.1 Confidentiality is an obligation for all staff. There is a Confidentiality clause in all staff's 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. In addition, any breach should be recorded as an incident within 72 hours to the Caldicott guardian.

5 Procedures

All staff must ensure that the following principles are adhered to: -

- 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 either your Line Manager or the Caldicott Guardians, Devan Moodley and Carmen Howarth-Tyler email inmind.caldicott@nhs.net or call 07557 807 003.
- All administration and clinical records, both manual and computer, must always remain at the unit unless authorised by the Registered Manager. All computer records are held under a Password system.
- Inmind Healthcare Group is responsible for protecting all the information it holds and must always be able to justify any decision to share information.
- Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.
- 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, with only certain staff having access to the keys as agreed with the registered Manager. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.
- Inmind Healthcare group promote a clear desk policy that all staff should adhere to always during and at the end of the day. They must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

- Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin.
- Inmind Healthcare Group use an external company that collect the secure waste bins who have their own confidentiality policy when disposing of the information

5 Disclosing Personal/Confidential Information

5.1 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.

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

5.3 Information can be disclosed: When effectively anonymising the information – password protecting documents with patient identifiable information included or using nhs.net accounts.

5.4 When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager before disclosing, who will inform and obtain approval of the Caldicott Guardians.

5.5 In identifiable form, when it is required for a specific purpose, with the individual's written consent.

5.6 In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their Line Manager before disclosing, who will inform and obtain the approval of the Caldicott Guardians.

5.7 Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail. Please seek advice from your line Manager regarding this principle.

6 Access to information

6.1 Users may have sight of Inmind Healthcare Group's records held in their name or that of their organisation. The request must be in writing to the Responsible Clinician giving the Responsible Clinician 28 days to respond and be signed by the individual. Once received by the Responsible Clinician they can authorise an administrator to act on this on their behalf.

6.2 The administrator must inform the Caldicott Guardians Devan Moodley and Carmen Howarth-Tyler.

6.3 Sensitive information will only be made available to the person or organisation named on the file.

6.4 Employees may have sight of their personnel records by giving 14 days' notice in writing to the Caldicott Guardians.

6.5 When photocopying or working on confidential documents, colleagues must ensure people passing do not see them. This also applies to information on computer screens.

7 Working Away from the Office Environment

7.1 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 Inmind Healthcare Group and service user information with them which could be confidential in nature e.g. on a laptop, secured USB stick or paper documents.

7.2 Taking home/ removing paper documents that contain person-identifiable or confidential information from Inmind Healthcare Group premises is discouraged.

7.3 To ensure safety of confidential information staff must keep them on their person always 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 always and kept in lockable locations.

7.4 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 Inmind Healthcare Group buildings. Confidential information is kept out of sight whilst being transported.

7.5 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.

7.6 If there is a breach this needs to be reported to Carmen Howarth-Tyler by email c.howarth-tyler@nhs.net or phone call 07557 807003 within 72 hours.

7.7 Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account.

7.8 Staff must not use or store person identifiable or confidential information on a privately-owned computer or device.

8 Information and Confidential Breaches

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

8.2 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.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.

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

8.4 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.

8.5 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.

8.6 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

8.7 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

8.8 You must also keep a record of any personal data breaches, regardless of whether you are required to notify. These need to be recorded on e-MDS within 72 hours as an incident.

9 Monitoring

Compliance with the policies and procedures laid down in this document will be monitored, together with independent reviews by both Internal Audits on a periodic basis.

10 Equality Impact Assessment

All relevant persons are required to comply with this policy. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals

11 Distribution and Implementation

11.1 This document will be made available to all Staff via the Inmind website and online training eLFY.

11.2 An email will be sent to all Staff notifying them of the release of this document. Together with a link for this document.

12 Associated Documents

The following websites will provide additional information:

Data Protection Act 1998 - *https://***www.gov.uk/data-protection**
Health & Social Care Act Regulation 20 – Records - *www.legislation.gov.uk/ukpga/2012/7/contents/en***act***ed*
Privacy and dignity – Human Rights Act - *https://www.liberty***humanrights***.org.uk/.../***human-rights-act**
Information Security - http://www.lawsociety.org.uk/support-services/advice/practice-notes/information-security/
The Common Law Duty of Confidentiality - *https://www.health-ni.gov.uk/articles/***common-law-duty-confidentiality**
GDPR - https://ico.org.uk/for-organisations/guide-to-the-general-data
The Computer Misuse Act (1990) - *https://www.legislation.gov.uk/ukpga/***1990***/18/contents*
The Caldicott Report (1997) - https://**www.gov.uk**/government/publications/the-information

Appendix A:

Acceptable Use Policy

1. Introduction

This document explains how the NHSmail service should be used. It is your responsibility to ensure you understand and comply with this policy. It ensures that:

- You understand your responsibilities and what constitutes abuse of the service.
- Computers and personal data are not put at risk.

As an NHSmail account holder, you should expect to receive ad-hoc communications about NHSmail from NHS Digital if you are based in England and National Services Scotland if you are based in Scotland informing you of changes or updates to the service that may impact your use.

If you have any questions about these terms and conditions, you should contact the NHSmail team at feedback@nhs.net (England) or nhsmail.scotland@nhs.net (Scotland) .

The NHSmail team reserves the right to update this document as necessary. A copy of the current version can be found at https://portal.nhs.net/Home/AcceptablePolicy

Supporting information can be found via the NHSmail support pages at: https://portal.nhs.net/Help/

2. General information about NHSmail

2.1 The NHSmail service includes the core services of secure email, the NHS Directory, Skype for Business Instant Messaging and Presence (IM&P), administration tools and a series of top-up services. The top-up services available to you will depend on your individual organisation.

2.2 The NHSmail services have been provided to aid the provision of health and social care and this should be your main use of the service.

2.3 There may be circumstances under which it is necessary for a designated and authorised person other than you, to view the contents of your files and folders within NHSmail. For example, if you have a secretary or PA that organises your diary.

2.4 If you are a member of clinical or care staff you may use NHSmail services in relation to the treatment of private patients in accordance with your own professional codes of conduct.

2.5 Health and social care staff contact details are provided in the NHS Directory to support the delivery of health and care - these details will be shared across the entire NHSmail health and social care community.

2.6 All data retained within the service remains the property of the NHS.

2.7 NHSmail accounts are owned by:

- NHS Digital (HSCIC) on behalf of the Secretary of State for Health in England
- NHS National Services Scotland (NSS) in Scotland

and are provided to NHS staff for their use. Where accounts are no longer used they are automatically removed after a period of inactivity as defined in the Data Retention Policy.

The NHSmail programme reserves the right to withdraw an NHSmail account from use should operational requirements dictate. This may include limiting service or complete de-activation.

3. Your responsibilities when using NHSmail

3.1 General responsibilities when using NHSmail:

3.1.1 You must not use NHSmail to violate any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is grounds for immediate dismissal and any illegal activity will be reported to the police. Illegal activity includes, but is not limited to, sending or receiving material related to paedophilia, terrorism, incitement to racial harassment, stalking, sexual harassment and treason. Use of the service for illegal activity will result in the immediate disablement of your NHSmail account.

3.1.2 You must not use any of the NHSmail services for commercial gain. This includes, but is not limited to: unsolicited marketing, advertising and selling goods or services.

3.1.3 You must not attempt to interfere with the technical components, both hardware and software, of the NHSmail system in any way.

3.1.4 When you set up your NHSmail account you must identify yourself honestly, accurately and completely.

3.1.5 You must ensure your password and answers to your security questions for the NHSmail services are always kept confidential and secure. You should notify your Local Administrator if you become aware of any unauthorised access to your NHSmail account. You must never input your NHSmail password into any other website other than nhs.net sites. You will never be asked for your NHSmail password. Do not divulge this information to anyone, even if asked.

3.1.6 Email messages are increasingly a source of viruses which often sit within attached documents. NHSmail is protected by anti-virus and anti-spam software although occasionally, as with any email service, a new virus or spam message may not be immediately detected. If you are unsure of the source of an email or attachment you should leave it unopened and inform your local IT services. If you receive spam messages you should forward them to spamreports@nhs.net. You must not introduce or forward any virus or any other computer programme that may cause damage to NHS or social care computers or systems. If you are found to be deliberately responsible for introducing or forwarding a programme that causes any loss of service, NHS Digital or National Services Scotland may seek financial reparation from your employing organisation.

3.1.7 You must not use the NHSmail service to disable or overload any computer system or network. Where excessive account activity is detected your account could be suspended, without notice, to safeguard the service for all other users.

3.1.8 All communication you send through the NHSmail services is assumed to be official correspondence from you acting in your official capacity on behalf of your organisation. This should be in accordance with your local organisation's policies for exchanging data. Should you need to, by exception, send communication of a personal nature you must clearly state that your message is a personal message and not sent in your official capacity. This includes Instant Messaging.

3.1.9 You must familiarise yourself with the NHSmail support pages which include important policy documentation, service status information, training and guidance materials, information about known issues with the service and user/administration guides.

3.1.10 If you are accessing your NHSmail account from a non-corporate device i.e. a home computer, personally owned laptop or in an internet cafe, you should only access the service via the web at www.nhs.net and not through an email programme such as Microsoft Outlook, unless you have explicit permission from your own organisation to do so.

3.2 Responsibilities when using the NHSmail email service:

3.2.1 You must not attempt to disguise your identity, your sending address or send email from other systems pretending to originate from the NHSmail service.

3.2.2 You must not send any material by email that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit or pornographic. If you need to transmit sexually explicit material for a valid clinical reason then you must obtain permission from your local Caldicott Guardian. [Note: GPs may need to refer to the Caldicott Guardian at their local CCG].

3.2.3 You must not use the NHSmail service to harass other users or groups by sending persistent emails to individuals or distribution lists.

3.2.4 You must not forward chain emails or other frivolous material to individuals or distribution lists.

3.2.5 It is your responsibility to check that you are sending email to the correct recipient, as there may be more than one person with the same name using the service. Always check that you have the correct email address for the person you wish to send to - this can be done by checking their entry in the NHS Directory.

3.2.6 Email is admissible as evidence in a court of law and messages can be classified as legal documents. Internal emails may also need to be disclosed under the Freedom of Information Act 2000, the Data Protection Act 1998 and amendments and Freedom of Information (Scotland) Act 2002. Emails should be treated like any other clinical communication and care should be taken to ensure that content is accurate, and the tone is appropriate.

3.3 Responsibilities when using the NHS Directory service:

3.3.1 It is your responsibility to make sure your details in the NHS Directory are correct and up to date.

3.3.2 You must not use the NHS Directory to identify individuals or groups of individuals to target for marketing or commercial gain, either on your behalf or on that of a third party.

3.4 Information governance issues:

3.4.1 The General Medical Council (GMC) Good Medical Practice guidance requires doctors to keep clear, accurate and legible records. It is important that emails and Instant Messages do not hinder this. You should ensure that relevant data contained in emails or Instant Messages are immediately attached to the patient record. Failure to do so could have implications on patient safety.

3.4.2 NHSmail is a communication tool to support the secure exchange of information and is not designed as a document management system. Documents, emails or messages that are required for retention/compliance purposes should be stored within your organisation's document management system in accordance with local Information Governance policies.

3.4.3 Your organisation is entitled to seek access to the contents of your mailbox, sent/received messages or other audit data as required to support information governance processes without your prior consent. Such requests are strictly regulated with the process detailed in the NHSmail support pages.

3.4.4 When moving your NHSmail account between health and care organisations, it is your responsibility to ensure any data relating to your role is archived appropriately and is not transferred to your new employing organisation in error. Guidance is available in the Leavers and Joiners section in the NHSmail support pages.

4. Using NHSmail services to exchange sensitive information

4.1 The NHSmail service is a secure service. This means NHSmail is authorised for sending sensitive information, such as clinical data, between NHSmail and:

- Other NHSmail addresses (i.e. from an '*.nhs.net' or '.hscic.gov.uk' account to an '*.nhs.net' or '.hscic.gov.uk' account)
- Other email systems that comply with the SCCI 1596 secure email standard
- Other email systems that comply with the pan-government secure email standard

4.2 If you need to exchange sensitive data outside of NHSmail or other email systems that do not comply with the SCCI 1596 secure email standard or the pan-government secure email standard, the NHSmail encryption tool must be used in accordance with the guidance materials available on the NHSmail support pages. Sending an email with [secure] in the subject line will automatically protect the message for you if you are unsure if the system you are sending to is secure or not.

4.3 If you intend to use the service to exchange sensitive information you should adhere to the following guidelines:

4.3.1 You should make sure that any exchange of sensitive information is part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated.

4.3.2 Caldicott and local Information Governance principles should apply whenever sensitive information is exchanged.

4.3.3 As with printed information, care should be taken that sensitive or personal information is not left anywhere it can be accessed by other people, e.g. on a public computer without password protection.

4.3.4 When you are sending sensitive information you should always request a delivery and read receipt (Email) or recipient acknowledgement (Instant Messaging) so that you can be sure the information has been received safely. This is especially important for time-sensitive information such as referrals.

4.3.5 You must not hold sensitive or personal data in your calendar if your calendar may be accessed by other people who are not involved in the care of that person.

4.3.6 If personal identifiable information is visible to other people, it is your responsibility to make sure those people have a valid relationship with the person.

4.3.7 You must always be sure you have the correct contact details for the person (or group) that you are sending the information to. If in doubt, you should check the contact details in the NHS Directory or use the search bar within IM&P.

4.3.8 If it is likely you may be sent personal and/or sensitive information you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.

4.4 Remember that personal information is accessible to the data subject i.e. the patient, under Data Protection legislation.

Appendix B:

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 NHS England.

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'ts

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.