Procedure Group: Information
Version no.: 1.3
Date of issue: May 2023
Approved by: Information Governance Group

Confidentiality Procedure

1. **Procedure purpose**
   The purpose of this Confidentiality Procedure is to lay down the principles that must be observed by anyone that has access to person-identifiable information or confidential information as part of their role.

   The information is often patient or staff member specific and may include personal health details or detail about other personal matters. However, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. Examples include employee records, occupational health records and confidential business information.

   The confidentiality of this information must be respected and maintained at all times. Everyone therefore is required to act in such a manner as to uphold the principle of confidentiality.

2. **Links to Policy**
   Data Protection Policy
   Data Protection Procedure
   Data Privacy Impact Assessment (DPIA) Procedure
   Personal Data Breach Reporting Procedure
   Subject Access Request (SAR) Procedure
   Privacy Rights Procedure
   Data Minimisation Procedure

   Policies and procedures available via the Policy A-Z:
   Policies - Policies - A-Z (sharepoint.com)

3. **Scope**
   This procedure applies to any individual who works for or on behalf of St Andrew's Healthcare. This includes St Andrew's Healthcare staff, agency workers, volunteers, contractors and third party organisations/individuals.

4. **Key requirements**
   There is a Confidentiality clause in staff contracts and St Andrew's Healthcare provides mandatory training which includes Data Protection and Confidentiality. All staff have to complete this training upon induction and then annually.

   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 a contract, and must be reported.

   Responsibilities

Everyone 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 person-identifiable information or confidential information must be discussed with the Information Governance (IG) Team or Caldicott Guardian.
- Minimisation techniques should be utilised to protect person-identifiable information, such as using pseudonyms, or anonymising the data to reduce the risk of data breach incidents. Guidance on data minimisation can be found in the Data Minimisation Procedure

Disclosing Personal/Confidential Information

When a request is received from an external organisation or when agreements with external organisations are being made to release person-identifiable information, or if there is a change to processing person- identifiable information, then approval should be sought from the Caldicott Guardian, where this relates to patients.

It is sometimes essential that we share person-identifiable information or confidential information at the right time with the right people. Sometimes this will be within St Andrew's Healthcare but also externally with other organisations, especially if we and other organisations are working together to support a patient or service user. This includes patient carers, family members, commissioners and regulatory bodies such as the Care Quality Commission.

Be open and honest with the person (and/or their carer/ family where appropriate) from the outset about why, what, how and with whom information will, or could be, shared. Further, seek their agreement, unless it is unsafe or inappropriate to do so

Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share person-identifiable information or confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden by one of the following reasons:

- Sharing the information is in the best interests of the person or others;
- We have a legal duty to share the information; or
- Sharing the information is in the interest of public safety/ national security.

Consider safety and wellbeing: base your information-sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions.

It is important to consider how much person-identifiable information or confidential information is needed before disclosing it. Only the minimal amount necessary should be disclosed. You may be able to share information by using data minimisation techniques which are further explained in the Data Minimisation Procedure.

Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what reason.

In most instances where we regularly share person-identifiable information or confidential information with an external organisation, an Information Sharing Agreement will need to be completed before any information is transferred. The agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements contact the IG team.

Sharing information securely

Care must be taken in transferring person-identifiable information or confidential information to ensure that the method used is as secure as it can be. Options for sharing information securely include:

- NHS Mail – NHS Mail is the most secure method for communicating and sharing person-identifiable information or confidential information to other secure email accounts.
- NHS Wales sharing portal – to be used to share information with NHS Wales regarding our NHS Wales patients only.
- Cryptshare – this is a sharing portal which can encrypt emails and documents. You can find further details on the intranet.
- St Andrew's Healthcare email – if sending person-identifiable information or confidential information via your email account do not put patient details within the subject header or full patient names in the body of the email. Any attachments must be password protected with a unique password and communicated separately.

Office Security

Take the following steps to prevent the loss and theft of person-identifiable information or confidential information in your work area:

- Do not let unauthorised people follow you through a locked door if they do not have a staff ID card or visitors pass.
- Minimise the amount of documents which contain person-identifiable information or confidential information on your desk.
- Immediately collect all print jobs and faxes that contain person-identifiable information or confidential information.
- Keep all computing devices, mobile devices, and other valuable items in a secure cabinet or drawer if they are not in use.
- Store paper documents in a locked drawer or filing cabinet at the end of each day.
- Lock your screen when you leave your desk.

Disposal of person-identifiable information or confidential information.
To dispose of documents that contain person-identifiable information or confidential information, put them in the confidential waste bins which are located across all areas of St Andrew's Healthcare

If you have a substantial amount of confidential waste that you need to dispose of you will need to raise a MICAD request through Estates and Facilities

IT equipment that has person-identifiable information or confidential information on it must be securely destroyed by IT.

Working away from the Office
You should always where possible avoid taking documents which contain person-identifiable information or confidential information out of the office. Carrying these documents can give rise to a data protection breach in a way that the theft of a St Andrew's Healthcare encrypted laptop (in the same circumstances) would not.

When documents containing person-identifiable information or confidential information are retained in St Andrew's Healthcare offices, there are numerous security measures to prevent unauthorised access. For instance, cabinets, drawers and doors can be locked, computers password-protected and data held on remote secure servers.

There are times when staff may need to take documents out of the Office, for instance if your role requires you to attend a hearing or tribunal.

When circumstances dictate that you do need to take paper documents which contain person-identifiable information or confidential information out of the office, it is less likely that you will be able to rely on the above safeguards. Therefore, you should bear in mind the following good practice points:

- Never needlessly transport documents off-site or from one site to another within St Andrew's Healthcare.
- Only take what is relevant and required in order to do the work that you need to do.
- Use a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of St Andrew's Healthcare buildings. This provides an extra level of security to protect those documents if they were to be lost or stolen.
- If you work from home you should be provided with an encrypted laptop which means that you can access your work and documents through the St Andrew's Healthcare VPN connection and need not actually take paper documents off site.

Carelessness
All staff have a 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.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.
- Forward any person-identifiable or confidential information via email to their personal e-mail account.
- Use or store person-identifiable or confidential information on a privately owned computer or device.
- Passwords must be kept secure and must not be disclosed to unauthorised persons.

Abuse of Privilege

It is strictly forbidden for staff to knowingly browse, search for or look at any person-identifiable 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.

Inappropriate access of a patient or service user's record without clinical, legal or operational justification, constitutes a breach of patient confidentiality. This may lead to disciplinary action for the staff member, and legal and regulatory consequences for St Andrew's Healthcare. Staff are reminded that access to patient records is monitored.

Professional Accreditation/Learning Development

There are times when certain Healthcare Professionals (Responsible Clinician, Approved Clinician and other professions) require to use healthcare reports that they have authored regarding their patients, for the purpose of professional accreditation or for learning and development needs.

If staff have a requirement to do this, they must either seek explicit and documented consent from the patient, using a consent form or they must ensure the report is anonymised to ensure that the patient cannot be identified from the information. Approval must also be sought from the relevant IPU Clinical Lead. If a patient gives consent for their healthcare reports to be used then the consent form must be uploaded onto the legal drop down tab in RiO.

5. **Monitoring and Oversight**

A failure to comply with the terms of the Data Protection Policy and the related Procedures may result in disciplinary action being taken against you, up to and including dismissal from St Andrew's Healthcare. For contractors, third parties or consultants non- compliance may result in termination of your contract.

The Data Protection Officer is responsible for the monitoring, revision and updating of this document on an annual basis or sooner if the need arises, together with independent reviews.

6. **Training**

St Andrew's Healthcare provides the following:

- Data Protection and confidentiality is included in the corporate induction session for all new starters.

- There is a mandatory e-Learning course which all staff have to complete upon induction and then annually.
- The IG Team can also provide face to face training sessions on request.

7. **References to Legislation and Best Practice**
This Procedure has been written in order to support St Andrew's Healthcare with compliance with the General Data Protection Regulation 2016/679 and the Data Protection Act 2018.

8. **How to request a change or an exception to this procedure**
Please refer to either the Policy and Procedure Update Application Link
Or the exception process Policy and Procedure Exception Application Link

9. **Key changes** - please state key changes from the previous version of the procedure

Version Number	Date	Revisions from previous issue
1.0	March 2019	Linked to Data Protection & Confidentiality Policy after Governance Review and reviewed and brought up-to-date. Approved at Information Governance Group
1.1	October 2019	Added Professional Accreditation section
1.2	April 2022	Minor changes on wording
1.3	May 2023	Extended review date by 12 months