PCIG Consulting

Policy on the Safe Transfer of Paper Records

Version: **1.0**

Date: **23 March 2020**

This template is for use by Practices to Comply with the GDPR requirement to have a policy regarding processing of patient data. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.

Change Control

Version	To	Change	Date
1			

Chapelgreen Practice

Policy on the Safe Transfer of Paper Records

Document History

Document Reference:	
Document Purpose:	Policy on the Safe Transfer of Paper Records
Date Approved:	
Version Number:	2.0
Status:	FINAL
Next Revision Due:	March 2021
Developed by:	Paul Couldrey – IG Consultant
Policy Sponsor:	Practice Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of Chapelgreen Practice or volunteering with the Practice.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2020

Equality Statement

This policy applies to all PRACTICE employees irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. All employees will be treated in a fair and equitable manner and reasonable adjustments will be made where appropriate, e.g. interpreter or signing provision, access arrangements, induction loop, etc.

The PRACTICE will ensure that this policy and guidance is monitored and evaluated by the Data Protection Officer.

1. Purpose

The purpose of this policy is to ensure the safety and confidentiality of paper records whilst they are in transit. Whilst the policy refers primarily to patient records it must be applied to all records containing person identifiable information (PCD Patient Confidential data) which will include Prescriptions also.

This policy covers how to ensure the security of records taken out on visits and how to safely transfer records between sites.

Records should spend the minimum amount of time in transit and should be delivered to their intended destination at the earliest opportunity.

If due to any medical emergency staff are taking paper records home to work from home this must be authorised using appendix one of the Mobile and Remote Working Policy 2020

2. Scope

This policy applies to all full time and part-time employees of the Practice, non-executive directors, contracted and third parties (including agency staff), students, trainees, secondees and other staff on placement with the Practice.

3. Information taken away from Practice premises

3.1 All staff must seriously consider the need for taking patient/client records out of their base with them on a visit. This should only happen when absolutely essential and there is no other method available for accessing/recording the information required. Staff must not carry around more information than is necessary.

3.2 It is recognised that health professionals may find it necessary to remove patient records from their base, to assist their daily practice of seeing patients in community settings. The guidelines below should be followed to reduce the risk of the records being accessed by an unauthorised person, lost or stolen.

When removing notes for home visits ensure that you take only for those visits that are pre booked. Consider whether you need the notes in order to carry out the visit? Records should not be removed for general administration purposes, e.g. writing routine reports. Record the removal and return of files taken away from the workplace. Records should be stored and carried in a secure bag/case. Records should not be carried 'loosely' as this increases the risk of dropping them and losing something. The bag/case used to store the records must never be left in a car when visiting but should accompany the member of staff on each visit/into each home.

Records must not be left in unattended cars, even if they are locked in the boot. If the member of staff is not returning to their base at the conclusion of their visits the records must be stored in the bag/case used and taken out of the car overnight into their home. Care must be taken in order that members of the family or visitors to the house cannot gain access to the records. This practice should only occur if the member of staff is not returning to their base after the working day or the records are required for the next working day. Staff must have the agreement of their manager if it is necessary for them to work in this way. Records should not be away from base for more than one working day i.e. if a member of staff is not returning to base at the conclusion of their working day, the records taken out on visits must be returned on their next normal working day.

There may be exceptional circumstances that means that this is not possible i.e. if a member of staff goes off sick before returning the notes. In this situation the records should be returned as soon as is practically possible. Managers may have to make arrangements to retrieve records if they are required whilst the member of staff is off for a period of time.

4. Transfer of records to other bases

4.1 Physical handover Where the record is related to significant events (e.g. complaints, legal action, access to records requests, serious incidents); or where the person holding the record or the person asking for it thinks that the record is particularly sensitive for other reasons, it should be delivered in person wherever possible.

4.2 External post - Royal Mail

When records are sent in the external post an assessment must be made as to the risk of loss. If the loss of those records could compromise patient care or create a serious breach of confidence the following procedure must be followed. It must be followed in all cases where whole patient records are being sent.

5. Tracking records

When an assessment has be made as to the risk of loss and the loss could compromise patient care or create a serious breach of confidence the following procedure must be followed. It must be followed in all cases where whole patient records are being sent so that their whereabouts are always known.

The person responsible for sending or taking records must log: The name and type of records removed, including any unique identifying number, The reason for removal and whether likely to be temporary or permanent if known, The date of removal,

The person the record is being sent / handed over to, Method of transfer, The date notified that the records have arrived at their destination including name of person confirming receipt, if appropriate. The date records return to base, if appropriate.

6. Monitoring and Review All breaches of this policy must be reported in line with the Practice Incident Reporting Policy.

On a routine basis a report on breaches of this policy shall be presented to the Data Protection Officer. The information will enable the monitoring of compliance and enable improvements to be made to the policy.