

## 1. Purpose

- 1.1. This policy sets out the procedure for the secure transfer, storage, access control, archiving and deletion of medical records and prepared chronologies between A1 Chronologies and its Clients (Instructing Parties).
- 1.2. It applies to all matters involving special category personal data, including medical records.
- 1.3. A1 Chronologies applies a proportionate file transfer model depending on whether the Client is managed under Model A (Repeat Instruction Clients) or Model B (Single Matter Clients).

## 2. Approved Platform and Method

- 2.1. All case materials are transferred and stored via an approved secure cloud operated under a business account.
- 2.2. The current platform used is Google Workspace hosted on European servers.
- 2.3. Two-factor authentication is mandatory for authorised users.
- 2.4. Medical records should not be sent via unsecured email attachment unless password-protected and agreed in advance. Informal transfer methods, including messaging applications, are not permitted.

## 3. Operational Models

- 3.1. A1 Chronologies operates two file transfer models:  
Model A – Repeat Instruction Clients (Section 4)  
Model B – Single Matter Clients (Section 5)
- 3.2. The appropriate model is determined based on the nature and anticipated frequency of instructions.

## 4. Model A – Repeat Instruction Clients

- 4.1. A dedicated secure shared workspace is established for Clients providing repeat or ongoing instructions.

4.2. A separate root folder is created for each Instructing Party, titled:  
“A1 Chronologies – [Client Name] – Secure File Transfer”

4.3. Within that folder, the following structure applies:

01 – “[Client Name] Uploads”

Purpose: Upload of instructions, medical records and supporting documents.

Permissions: Client – Editor; A1 Chronologies – Editor

02 – “A1 Chronologies Uploads”

Purpose: Delivery of completed chronologies and any authorised revisions.

Permissions: Client – Viewer; A1 Chronologies – Editor

03 – “Archived”

Purpose: Storage of completed matters during the retention period.

Permissions: Client – Viewer; A1 Chronologies – Editor

4.4. Case Folder Naming Convention

Each matter is organised within its own case folder using the following format:

Patient Last Name, First Initial – A1C Reference

4.5. File Naming Convention

Chronology documents must follow the format:

YYYY-MM-DD Chronology – Patient Last Name, First Initial

YYYY-MM-DD Summary – Patient Last Name, First Initial

Where amendments are made following delivery, a new document is issued using the same naming format with the updated date. The most recent dated document represents the current operative version. Descriptors such as “final”, “revised”, “new” or “latest” are not used.

#### 4.6. Case Lifecycle

**New Instruction:**

A case folder is created within “Client Uploads” and mirrored within “A1 Chronologies Uploads”. The Client uploads medical records and instructions to the relevant folder.

**Preparation:**

All drafting and working documents remain internal and are not shared.

**Delivery:**

The completed chronology is uploaded to the relevant case folder within “A1 Chronologies Uploads”. The Client is notified by email.

**Closure:**

Once the matter is complete and no further amendments are required, the case folder is moved to “Archived”. Any amendments following archiving require written confirmation before reactivation.

#### 5. Model B - Single Matter Clients

- 5.1. For single matters or first-time instructions where ongoing work is not yet established, a simplified secure transfer process is used.
- 5.2. Upon confirmation of instruction, a secure upload folder is created and shared with the Client for the sole purpose of uploading medical records and instructions.

Titled: “A1 Chronologies – [Client Name] – Secure File Upload”

Permissions: Client – Editor; A1 Chronologies – Editor

- 5.3. Upon completion of the chronology, a separate secure delivery folder is created and shared containing the completed chronology and summary.

Titled: “A1 Chronologies – [Client Name] – Secure File Delivery”

Permissions: Client – Viewer; A1 Chronologies – Editor



[a1chronologies.co.uk](https://a1chronologies.co.uk)

Excipian Ltd. (Trading as A1 Chronologies)  
Registered in England & Wales | Company No. 06913406  
Registered Office: 124 City Road, London, EC1V 2NX

- 5.4. Documents within the delivery folder must follow the same file naming convention as set out in section 4.5:

Parent Folder:

Patient Last Name, First Initial | A1C Reference

Documents within the folder:

YYYY-MM-DD Chronology – Patient Last Name, First Initial

YYYY-MM-DD Summary – Patient Last Name, First Initial

Where amendments are required, a new document is issued using the same format with the updated date. The most recent dated document represents the current operative version.

- 5.5. Following confirmation of delivery, the upload folder may be restricted or removed where appropriate.
- 5.6. If further instructions are received from the same Client, the arrangement may transition to Model A.

## **6. Retention and Deletion**

- 6.1. For shared workspaces established under Model A or Model B, Client access will ordinarily be removed 30 days after invoice settlement, unless otherwise agreed in writing.
- 6.2. A1 Chronologies retains internal archived copies of completed case files for a period of six (6) years from the date of settlement of the matter or the date of last correspondence between the parties in relation to that matter, whichever is later.
- 6.3. Internal archived files are stored securely and are not accessible to the Client following removal of shared workspace access.
- 6.4. At the expiry of the applicable retention period, archived files are permanently deleted unless continued retention is required for legal, regulatory, or accounting purposes.

## **7. Security and Access Control**

- 7.1. Access is restricted to named individuals authorised by the Client.



[a1chronologies.co.uk](https://a1chronologies.co.uk)

Excipian Ltd. (Trading as A1 Chronologies)  
Registered in England & Wales | Company No. 06913406  
Registered Office: 124 City Road, London, EC1V 2NX

- 7.2. Personal email accounts are not used to access sensitive case materials.
- 7.3. Downloads to local devices are permitted only where devices are password-protected and encrypted.
- 7.4. A1 Chronologies reserves the right to review and amend access permissions where necessary to maintain data security.

## **8. Periodic Review**

Access permissions and folder structures are reviewed periodically to ensure:

Active matters are clearly separated from archived matters.

Access rights remain appropriate.

Retention periods are applied consistently.

## **9. Policy Review**

9.1. This policy may be updated periodically to reflect operational or regulatory requirements.

9.2. The current version applies to all instructing parties unless otherwise agreed in writing.