



## CDISC Policy 007

# Record Retention and Destruction

### Revision History

<b>Date</b>	<b>Revision</b>	<b>Description</b>	<b>Author</b>
July 2016	0.1	Original Draft	Governance Committee
03 November 2016	1.0	Approved	CDISC Board of Directors
13 December 2018	2.0	Revision	CDISC Legal Advisors
May 2019	2.0	Approved	CDISC Board of Directors
October 2023	2.0	Approved – no changes	CDISC Board of Directors

## CDISC PERSONAL DATA RETENTION POLICY

### 1. ABOUT THIS POLICY

- 1.1. This Personal Data Retention Policy (**this Policy**) sets out how long CDISC will retain personal data and explains how CDISC complies with the data retention rules contained within the European Union General Data Protection Regulation (**GDPR**) and other applicable data protection and privacy laws (collectively, **Data Protection Laws**).
- 1.2. This Policy should be read together with the CDISC Data Protection Policy and any other CDISC policies relating to information security and risk management which CDISC may implement from time to time. If you have any questions regarding this Policy, please contact a member of CDISC Data Privacy Committee.

### 2. OUR RETENTION OBLIGATIONS

- 2.1. Storage limitation is one of the Data Protection Principles set out in the GDPR. Article 5(1)(e) of the GDPR states:

*“Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.”*

- 2.2. CDISC must always be able to justify how long CDISC keeps personal data which it controls (**CDISC Personal Data**). If CDISC no longer has any purposes for which it needs to process CDISC Personal Data then it should be deleted or ‘anonymised’ (by removing any information from the personal data which makes the individual identifiable). Where it is not possible technically to delete all traces of data, the key issue is to ensure that the data is put beyond use.
- 2.3. This means CDISC will not retain CDISC Personal Data indefinitely “just in case” (or if there is only a small possibility) that it may use those data in future.
- 2.4. CDISC also maintains a personal data Retention Schedule which records various details relating to the different types of CDISC Personal Data which CDISC processes in connection with CDISC’s business. The Retention Schedule sets out specific retention periods for each type of CDISC Personal Data. The Retention Schedule also lists the retention period for information which is not necessarily CDISC Personal Data (because it is not ‘personal data’), but which is still information or data controlled by CDISC.

### 3. HOW CDISC SETS RETENTION PERIODS

- 3.1. Data Protection Laws do not dictate mandatory retention periods, and so it is CDISC’s responsibility to determine appropriate retention periods based on the fundamental principle that CDISC must be able to justify why CDISC is retaining the data.
- 3.2. In determining the retention periods in the below Retention Schedule, CDISC takes into account all relevant factors, including:
  - **Purpose:** how long CDISC will need to retain the data for the purpose(s) for which it was obtained.

- **Record:** whether CDISC needs to retain a record of CDISC's relationship with an individual once that relationship with them has ended, but delete all other information.
  - **Legal claims:** whether CDISC needs to keep information to defend possible future legal claims.
  - **Legal or regulatory requirements:** CDISC will have a valid reason to retain data wherever necessary to comply with applicable legal or regulatory requirements such as tax laws and health & safety requirements.
  - **Industry standards and guidelines:** these can be a useful starting point for determining retention periods but must still be treated with caution as they do not guarantee compliance.
- 3.3. Documents and financial files that are essential to keeping CDISC operating in an emergency will be duplicated or backed up at least every week and the duplicate/back-up copies will be maintained off-site.
- 3.4. Electronic documents will be retained as if they were paper documents. Therefore, any electronic files that fall into one of the document types in the Schedule will be maintained for the amount of time set out therein.

#### **4. ALTERNATIVE OPTIONS TO DELETION OR ANONYMISATION**

- 4.1. Where there is no longer a purpose for processing CDISC Personal Data, but there is a reasonable likelihood that such data will be required in future in a form which permits identification of individuals, then it should be considered whether, as an alternative option to deletion or anonymisation, the data should be archived or pseudonymised.
- 4.2. It is important to note that archived or pseudonymised data is still regulated as personal data and must be handled in compliance with Data Protection Laws.

#### **5. DESTRUCTION OF CDISC PERSONAL DATA**

- 5.1. Each department within CDISC is responsible for the continuing process of identifying the CDISC Personal Data that have met their required retention period and supervising their destruction.
- 5.2. The destruction of CDISC Personal Data and any confidential or financial information records stored in paper format is to be conducted by secure shredding. The destruction of electronic records is to be carried out in a secure manner that makes the information irretrievable (including the physical destruction of obsolete media, such as hard disks, and the overwriting of electronic data).
- 5.3. CDISC recognise that there may be instances where records containing personal data must be kept for longer than the relevant retention period. Therefore the date of destruction for records containing personal data may be suspended if a claim, audit, investigation or lawsuit has been threatened or filed by or against CDISC or is reasonably foreseeable.

- 5.4. On learning of an actual or reasonably anticipated legal action, the CEO will notify relevant staff to suspend disposal and destruction of applicable records. This is known as a **'legal hold'**.
- 5.5. If someone becomes aware of an actual or anticipated claim, audit, investigation or litigation, they must immediately report the matter to the Data Privacy Committee and discontinue any scheduled disposal pending confirmation of whether a legal hold is required.
- 5.6. It is important not to alter, dispose of, discard or destroy any records that are subject to a legal hold. Staff must also continue to retain any and all such records until the CEO issues a notice indicating that the legal hold has been lifted and that the retention and disposal of such records should resume in accordance with the retention schedule.
- 5.7. In the event of a data subject request ("**DSR**"), such as a data subject access request, the personal data which is the subject of the DSR should be retained (in the same manner as if a legal hold were applied) to the extent required in order to fulfil the DSR.

**6. QUERIES**

If you have any queries regarding the retention of CDISC Personal Data then please contact the Data Privacy Committee.

**7. IMPLEMENTING AND UPDATING THIS POLICY**

The Data Privacy Committee will oversee the implementation of this policy by CDISC and will review and update it periodically.

**8. AUTHORIZATION**

This document has been approved and is in effect on this date:

Name	Date
CDISC Board of Directors	October 17, 2023

## CDISC RETENTION SCHEDULE

File Category	Item	Retention Period
<b>Corporate Records, Finance and Administration</b>	Bylaws and Articles of Incorporation	Permanent
	Corporate resolutions	Permanent
	Board and committee meeting agendas and minutes	Permanent
	Conflict-of-interest disclosure forms	4 years
	Financial statements (audited)	Permanent
	Auditor management letters	Permanent
	Payroll records	7 years
	Check register and checks	Permanent
	Bank deposits and statements	7 years
	Chart of accounts	7 years
	General ledgers and journals (includes bank reconciliations)	7 years
	Investment performance reports	7 years
	Equipment files and maintenance records	7 years after disposition
	Contracts and agreements	7 years after expiration/termination and after all obligations end
Correspondence – general	7 years	
<b>Grant records</b>	Contribution Records	Permanent
	Documents Evidencing Terms of Gifts	Permanent
	Grant Records	7 years after completion of grant period or date of grant if for general operating support
<b>Insurance Records</b>	Policies – occurrence type	Permanent
	Policies – claims-made type	Permanent

	Accident reports	7 years (if no claim)
	Safety (OSHA) reports	7 years following the calendar year covered by the report
	Claims (after settlement)	20 years after closure of claim
	Group disability records	7 years after end of benefits
<b>Real Estate</b>	Deeds	Permanent
	Leases (expired)	7 years after all obligations end
	Mortgages, security agreements	Permanent
<b>Tax</b>	IRS exemption determination and related correspondence	Permanent
	IRS Form 990s	Permanent
	Charitable Organizations Registration Statements	Permanent
<b>Human Resources</b>	Employee personnel files	Duration of employment plus 6 years
	Retirement plan benefits (plan descriptions, plan documents)	Plan life plus 6 years
	Employee handbooks	10 years after superseded
	Workers comp claims (after settlement)	10 years
	IRS Form I-9	Greater of 1 year after end of service, or three years
	Withholding tax statements	7 years
	Timesheets	5 years
<b>Technology</b>	Software licenses and support agreements	7 years after all obligations end