CDISC Policy 011

Personal Data Breach Notification

Revision History

Date	Revision	Description	Author
December 2018	1	Original Draft	CDISC Legal Advisors
May 2019	1	Approved	Board of Directors

PERSONAL DATA BREACH NOTIFICATION POLICY

1. ABOUT THIS POLICY

1.1. This Breach Notification Policy (**this Policy**) sets out how and when CDISC will notify third parties and/or regulatory authorities in the event of a personal data breach.

1.2. This Policy is intended to protect CDISC, its members (and other third parties involved with CDISC) and individual data subjects and to help CDISC comply with European Union General Data Protection Regulation (**GDPR**) and other applicable data protection and privacy laws (collectively, **Data Protection Laws**).

1.3. All CDISC staff (whether directors, officers, employees, consultants, contractors, temporary and agency workers and other staff - together **Staff**) must follow the procedures set out in this Policy in the event of a personal data breach.

1.4. As set out in Section 4 of the CDISC Data Protection Policy, CDISC may not always be directly regulated by GDPR. In these cases, where a personal data breach does occur, the Data Privacy Committee will determine the appropriate course of action, taking into consideration the best interests of CDISC, its members and the affected individuals.

2. IDENTIFYING A PERSONAL DATA BREACH

2.1. A personal data breach is: "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*"

2.2. In practice, this means a security incident arising which affects the confidentiality, integrity or availability of personal data. Common examples include:

- A cyberattack resulting in personal data being unlawfully accessed, disclosed or made unavailable.
- A ransomware attack making personal data unavailable by encrypting it.
- Loss of the decryption key for encrypted personal data.
- Loss or theft of devices on which personal data are stored or can be accessed, such as mobile phones, laptops, tablets, USB sticks and hard drives.
- Loss or theft of confidential documents or files containing personal data.
- Sending emails containing or attaching personal data to the wrong recipients.
- CC'ing instead of BCC'ing email recipients.
- Making personal data accessible on the public internet.
- Someone gaining unlawful access to personal data.
- Not removing personal data from documents intended to be anonymised.
- A breach by one of our suppliers, who processes personal data on our behalf.

3. CDISC's RESPONSIBILITIES AS CONTROLLER AND AS PROCESSOR

3.1. Data protection law draws a distinction between a **data controller**, which decides how and why personal data is processed, and a **data processor**, which processes personal data on behalf of a data controller.

3.2. CDISC is a data controller in respect of personal data it controls (**CDISC Personal Data**), for example information about CDISC's staff, contractors, business contacts (including individual representatives of members and other corporations CDISC deals with).

3.3. CDISC acts as a data processor where CDISC is processing personal data on behalf of our members or other third parties (**Member Personal Data**).

3.4. In situations where CDISC is regulated by GDPR (see Section 4 of the CDISC Data Protection Policy for further details) CDISC may have to report a personal data breach to an EU supervisory authority and, potentially, the affected individuals (if CDISC is a controller) or to the relevant member or other controller (if CDISC is a processor).

3.5. There can also be very serious consequences for individuals working for CDISC who cause a personal data breach, particularly if the breach was the result of misconduct by the person involved. For example, if a member of Staff took copies of one of CDISC databases without permission or unlawfully disclosed or sold CDISC personal data then this could lead to them personally being prosecuted and fined or, in extreme cases, imprisoned.

3.6. **All Staff who become aware of a personal data breach must immediately report it to CDISC's Data Privacy Committee.** The Data Privacy Committee will then determine if and how the breach should be reported.

4. REPORTING A BREACH

4.1. When a security incident takes place, CDISC must establish: (a) whether a 'personal data breach' (as set out in Section 2.1) has occurred; (b) the likelihood and severity of the risk to individuals' rights and freedoms; and (c) if the personal data is CDISC Personal Data and/or Member Personal Data.

5. BREACHES RELATING TO CDISC PERSONAL DATA

5.1. In situations where the GDPR applies due to its extra territorial effect, CDISC may have to report the matter to a European Union data protection supervisory authority. The appropriate authority will depend on a range of factors including where the breach occurred and who was primarily affected. However, such a report is only required if the security incident can be considered to be a '*personal data breach'* (as defined in Section 2.1) **and** it poses a risk to individuals' rights and freedoms

5.2. If the data breach is subject to GDPR **and** it is likely that there will be a risk to the affected individuals, then CDISC must notify the supervisory authority without undue delay, but not later than 72 hours after becoming aware of it. If CDISC takes longer than this, CDISC must give reasons for the delay and supply the relevant information as soon as it becomes available. If it is not possible to provide all of the necessary information at the same time, CDISC will have to provide the information in phases (without undue delay).

5.3. In each case CDISC should consider all relevant factors to assess the potential negative consequences for individuals from the perspective of potential emotional distress and of

physical and material damage. These may include: (a) psychological distress; (b) humiliation or damage to reputation; (c) discrimination; (d) being exposed to physical harm or violence; (e) identity theft or fraud; (f) financial loss.

5.4. Technical factors such as whether the CDISC Personal Data was securely encrypted and backed up will also be important in establishing if a risk exists. CDISC will therefore need the full support of the persons involved to ascertain as much information as possible regarding the security incident as quickly as possible.

6. NOTIFICATION TO AFFECTED INDIVIDUALS (CDISC PERSONAL DATA)

6.1. If the personal data breach falls within the scope of the GDPR and it is likely to result in a high risk to the rights and freedoms of the data subject then CDISC must notify the data subjects affected immediately.

6.2. A template letter for notifying individuals is attached as Appendix 1. The notification could also be made by email. If it is not possible or would be disproportionate to contact each individual, then a public notice (e.g. on our website) may suffice.

6.3. CDISC is not required to notify the individual under GDPR if: (a) measures have been taken to render the CDISC Personal Data unusable (e.g. encryption); or (b) measures are subsequently taken which will ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.

7. NOTIFICATION TO MEMBERS (MEMBER PERSONAL DATA)

Under Data Protection Laws CDISC may be required to notify Members after becoming aware of any personal data breach in relation to Member Personal Data. Under GDPR, this notification must be made without undue delay.

8. DOCUMENTING DATA BREACHES

The Data Privacy Committee will record details of all personal data breaches, regardless of whether or not they are reported, in CDISC's Register of Data Breaches (Appendix 2)

9. IMPLEMENTING AND UPDATING THIS POLICY

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

10. AUTHORIZATION

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

Name	CDISC Board of Directors
Date	6 May 2019

APPENDIX 1

TEMPLATE BREACH NOTIFICATION LETTER TO AFFECTED DATA SUBJECTS

[On CDISC headed notepaper]

[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE/ZIPCODE]

[DATE]

Dear [NAME],

Notification of a personal data breach

We are sorry to inform you of a breach of security that has resulted in the [loss of **OR** unauthorised disclosure of **OR** unauthorised access to **OR** alteration of **OR** destruction of **OR** corruption of] your personal data.

The breach was discovered on [DATE] and is likely to have taken place on or around [DATE].

As a result of our investigation of the breach, we have concluded that:

- The breach affects the following types of information:
    - [TYPES OF INFORMATION, FOR EXAMPLE, FINANCIAL, SPECIAL CATEGORY DATA, CRIMINAL OFFENCE DATA].
- The information has been [accidentally or unlawfully destroyed OR corrupted OR lost OR altered OR disclosed without authorisation OR accessed by [[NAME OR DESCRIPTION OF ORGANISATION] OR an unauthorised person]].

The breach occurred under the following circumstances and for the following reasons:

- [CIRCUMSTANCES].
- [REASONS].

We have taken the following steps to mitigate any adverse effects of the breach:

- [MEASURES].

We recommend that you take the following measures to mitigate possible adverse effects of the breach:

- [MEASURES].

[We informed the Information Commissioner's Office of the breach on [DATE].]

You can obtain more information about the breach from any of the following contact points:

- [GOVERNANCE COMMITTEE CONTACT DETAILS]

We apologise for any inconvenience this breach may cause you.

Yours sincerely,

[NAME]

For and on behalf of the Clinical Data Interchange Standards Consortium

APPENDIX 2
CDISC REGISTER OF PERSONAL DATA BREACHES

Date of breach	Nature of the breach	Description of the breach	Personal data affected (Type + CDISC PD or Member PD)	No of data subjects affected	No of data records affected	Details of CDISC's point of contact for information about the breach	Consequences of the breach	All individuals informed?	Remedial action	Date of remediation completed	Other information