Daten-Sicherheit

Dokument Nummer	CIO-DM-005-00	**Autor**	G Antony
Versions Nummer	3.2	**Reviewer**	E Sauer
Vorige Version	3.1	**Review**	18-Jul-2024
Tritt in Kraft am	01-Aug-2024	**Status**	Final

Inhaltsverzeichnis

1. Allgemeine Informationen

1.1. Ziel und Umsetzung

- Das Ziel dieses Verfahrens ist es alle Schlüsselaspekte der Informationssicherheit zu definieren. Das Ziel ist es nicht eine Arbeitsweise Schritt für Schritt zu spezifizieren, sondern lediglich einen Rahmen zu erstellen, in dem eine Arbeitsanleitung entwickelt werden kann.

1.2. Gesetzgebung und Standards

- Für klinische Studien basieren die Minimalstandards auf ICH-GCP (http://www.ich.org/)
- Good Clinical Practice (GCP) ist ein internationaler, ethischer und wissenschaftlicher Qualitätsstandard zur Entwicklung, Durchführung, Dokumentierung und Berichterstattung von Studien, welche die Teilnahme von Menschen als Testsubjekte umfassen.

- Einhaltung dieses Standards versichert öffentlich, dass die Rechte, die Sicherheit und das Wohlergehen der Studienteilnehmer geschützt werden und die Daten der klinischen Studie glaubwürdig sind.

- Für elektronische Datenerfassung definiert 21 CFR Teil 11 die Kriterien, unter welchen elektronische Aufnahmen und Signaturen vertrauenswürdig, glaubwürdig und Papieraufzeichnungen als ebenbürtig angesehen werden.

- Für nichtklinische Studien werden die Minimalstandards von Studie zu Studie, risikenbasiert , mit Zustimmung des Vorsitzenden der die Studie durchführenden Organisation, des Projektleiters der Studie und des verantwortlichen Daten-Managers bei CIO entschieden, während das allgemeine Ziel der Datensicherung vom Quelldokument bis zur Datenbanksperre eingehalten wird.

- Falls örtliche Gesetzgebung zusätzliche Standards des DM fordert, müssen diese übernommen werden.

2. Verantwortlichkeiten

Rollen	Verantwortlichkeit
Projektleiter	- Unterstützt das Projektteam bei der Identifizierung und Implementierung von Lösungen von Daten-Management-Problemen und Bedenken des DM und des Teams - Bewilligt die SOP Daten Sicherheit und hilft bei ihrer Entwicklung und Pflege - Stellt sicher, dass regelmäßig eine Kontrolle der Daten-Management-Aktivitäten durchgeführt wird - Beaufsichtigt das Testen des Daten-Management-Systems, Bearbeitungs-/Validierungs-Checks und spezielle Listen/Verfahren, die als Werkzeuge für Daten-Review und Diskrepanz-Management Aktivitäten genutzt werden. - Beaufsichtigt die Erstellung von Daten-Management-Plänen und Qualitätsmanagementplänen, um genaue, pünktliche, konsistente Qualitätsdaten zu liefern - Stellt sicher, dass Daten-Management-Werkzeuge sicher und passend in Hinsicht auf die Daten-Management-Aspekte des Projekts sind.
Leiter der Daten-Management-Abteilung	- Überwacht und bewilligt Informationssicherheitsverfahren

Rollen	Verantwortlichkeit
Daten-Manager	- Erhält die Genauigkeit, Integrität und Sicherheit von komplexen, umfangreichen, computerisierten Daten-Management-System - Erhält die Vertraulichkeit der Daten gemäß den Projektanforderungen - Definiert die Zugangsniveaus der Daten für die Nutzer der Studie - Verwaltet die Nachverfolgung von Daten bei Übertragungen - Verhindert jegliche Hinzufügungen, Löschungen oder Änderungen des Audit Trail außer durch das System - Reguliert Passwort- und Nutzerverwaltungsänderungen - Stellt sicher, dass Backup Pläne gemäß dem Zeitplan ausgeführt werden
Dateneingabeangestellter	- Führt Prozesse der Informationssicherheit aus
Datenmonitor	- Überwacht Sicherheits- und Backupsysteme während der Studie
Systementwickler	- Implementiert soweit möglich Informationssicherheit in das entwickelte System ein

3. Definitionen und Abkürzungen

Definition

- **Information** - Information kann viele Formen annehmen. Für die Zwecke dieser Richtlinie umfasst der Begriff Daten, die auf Computern gesichert sind, die über Computernetzwerke transferiert werden, gedruckt, aufgeschrieben, per Post oder Fax gesendet werden oder auf externen Geräten gespeichert werden. Ein Großteil dieser Richtlinie bezieht sich speziell auf elektronische Informationen, aber dieselben Prinzipien und derselbe Grad an Sorgfalt sollte für papier-basierte Informationen verwendet werden. Informationen können entweder einem definierten Format nach strukturiert oder unstrukturiert sein.

- **Informationsressourcen** - Informationsressourcen umfassen Informationen (s. oben), Computersoftware und Hardware

- **Zugang und Sicherheit** - Zugang beschreibt jeden Mechanismus, durch den Personen Zugang zu Informationen erhalten. Diese Richtlinie definiert legitimen Zugang und schreibt vor, wie mit unautorisiertem Zugang umzugehen ist.

- **Sicherheit** - Sicherheit beschreibt Mechanismen und Verfahren, die sicherstellen, dass angemessene Kontrollen für den Informationszugang vorhanden und effektiv sind.

- **Vertraulichkeit** - Vertraulichkeit erfordert die Sicherung von Daten vor unautorisierter Offenlegung oder Abfangen in lesbarer Form (s. unten)

- I**ntegrität** - Integrität involviert den Schutz der Genauigkeit, Vollständigkeit und Einheitlichkeit von Informationen und Computersoftware

- **Verfügbarkeit** - Verfügbarkeit umfasst, dass Informationen und zugehörige Dienste zur Verarbeitung der Informationen für das Personal und Studenten soweit notwendig verfügbar sind.

- **Computersoftware** - Computersoftware ist die Sammlung von Computerprogrammen, die zur Verarbeitung von Informationen genutzt werden.

- **Verständliches Abfangen** - Verständliches Abfangen ist das Abfangen von Informationen in einer Weise, dass sie lesbar sind. Verschlüsselung von Daten kann genutzt werden, um verständliches Abfangen zu verhindern.

Abkürzungen

• DM	Data Management (Daten-Management)
• PI	Principle Investigator (Prüfleiter)

4. Methode

- Die Hauptziele einer Richtlinie zur Datensicherheit und zugehörigen Aktivitäten sind die Vermeidung von Verlust oder Schaden an Studiendaten und die Erhaltung der Daten-Management-Einrichtungen im bestmöglichen Zustand.

- Ein voller Review des Prozesses, der effektiven Informationszugang und Sicherheitskontrolle sicherstellt, sollte mit folgenden Ergebnissen ausgeführt werden:

  - Informationsressourcen sind identifiziert und passend geschützt

  - Informationsnutzer sollten identifiziert sein und Zugang zu den Informationen, für die sie autorisiert sind, haben - zum Beispiel zur Datenbankverwaltung

  - Regelmäßiger Review der Nutzerzugangsrechte. (Siehe Informationsbestand Register)

  - Daten-Management-Systeme sind angemessen verwaltet und kontrolliert

- Der Prozess sollte Folgendes enthalten:
  - Nutzerregistrationsverfahren, Authentifizierungsmechanismen und Passwortnutzung für Zugang zu jeglichen Computersystemen oder Einrichtungen,
  - Systempatches und Antivirus Schutz
  - Systemsicherheitsverfahren, inklusive Systemverwaltung, Überwachung und Protokollierung,… (siehe Vereinbarung zur Vertraulichkeit und zum Nutzerverhalten)
  - Backup der Computersysteme, Definition, wie lange Backups vorgehalten werden (Aufbewahrungszeitraum), Häufigkeit, Medium (USB, PC, Server,…) und on-site/off-site Vorkehrung
  - Inventar von Informationsressourcen, inklusive Zubehör, Software und Daten in Papier und digitaler Form.
  - Systemänderungskontrolle, Test und Akzeptanz
  - Risikoeinschätzung für Desaster Recovery gemäß verfügbaren Ressourcen
  - Physische Sicherheit der Computerräume, Netzwerke, PCs; Instandhaltung und Entsorgung der Rechner
  - Audit Trail zur Kontrolle der Eingabe und Änderung von Dokumenten und Studiendaten

5. Anhänge und Formulare zur Vervollständigung

- Anhang 1: Vorlage Informationsbestand Register

- Anhang 2: Vorlage Vereinbarung zur Vertraulichkeit und zum Nutzerverhalten

6. Verweise auf andere SOPs

Dieses SOP konzentriert sich auf Systemvalidierung und sollte zusammen mit Folgenden SOPs gelesen werden:

- CIO-DM-001-00-SOP-Allgemeines-Daten-Magement

- CIO-DM-003-00-SOP-Datenbank-und-eCRF-Entwicklung

- CIO-DM-008-00-SOP-Datenerhebung-und-Dateneingabe

- CIO-DM-012-00-SOP-Daten-Nachverfolgung

7. Genehmigung und Verbreitung

	Name und Funktion
Initiiert von:	Gisela Antony, Leiterin CIO Marburg
Überarbeitet von:	Edda Sauer, CIO Marburg Personal
Manuelle Verbreitung:	Nur für momentanen Druck bestimmt

8. Referenzen

- ISO 27001 - http://www.27000.org/iso-27001.htm