Aufbewahrung und Archivierung von Personaldaten

## Zweck

Diese SOP beschreibt die Verfahren zur Aufbewahrung und Archivierung von Personendaten, um die gesetzlichen Anforderungen zu erfüllen und den Datenschutz zu gewährleisten.

## Geltungsbereich

Diese SOP gilt für alle Mitarbeiter von Viva Hub AG, die mit der Erfassung, Verarbeitung und Aufbewahrung von Personendaten betraut sind.

## Verantwortlichkeiten

- Datenschutzbeauftragter Überwachung der Einhaltung der SOP und regelmäßige Schulung der Mitarbeiter.

- Mitarbeiter Einhaltung dieser SOP und Meldung von Abweichungen oder Sicherheitsvorfällen an den Datenschutzbeauftragten.

## Aufbewahrungsfristen

Die folgenden gesetzlichen Aufbewahrungsfristen sind einzuhalten

- Krankengeschichten 20 Jahre nach Abschluss der jeweiligen Behandlung (Art. 60 Abs. 1bis und 2 OR).

- Dokumentation von Strahlenanwendungen 20 Jahre für Expositionsparameter, 10 Jahre für Anwendungen im mittleren und Hochdosisbereich sowie Mammografie (Art. 20 Abs. 5 RöV).

- Dokumentation des Umgangs mit Blutprodukten 30 Jahre (Art. 39 und 40 HMG).

- Dokumentation des Umgangs mit Organen, Geweben oder Zellen 20 Jahre (Art. 34 und 35 Transplantationsgesetz).

- Arbeitsmedizinische Dokumente 40 Jahre (Art. 8 Anhang 4 zur Standesordnung der FMH).

- Personaldossiers 5 Jahre ab Austritt des Mitarbeitenden (Art. 330a OR).

- Rechnungen und Steuerunterlagen 10 Jahre (Art. 958 und 958f OR).

## Technische Anforderungen

- Sichere Aufbewahrung Personendaten sind in verschlossenen Aktenschränken oder gesicherten digitalen Systemen aufzubewahren. Der Zugang ist auf berechtigte Personen zu beschränken.

- Schutz vor Umwelteinflüssen Datenträger sind vor Wasser, Feuer und anderen Umwelteinflüssen zu schützen.

- Digitale Formate Digitale Daten sind in archivierungstauglichen Formaten (z.B. PDFA, TIFF) aufzubewahren und regelmäßig zu aktualisieren.

- Back-ups Regelmäßige Back-ups sind durchzuführen und mindestens einmal jährlich zu testen.

## Vernichtung von Daten

- Physische Vernichtung Mechanische Zerstörung von Datenträgern (z.B. Schreddern).

- Magnetische Löschung Nutzung spezieller Löschgeräte für Festplatten.

- Technisches Überschreiben Mehrmaliges Überschreiben von Daten mit zufälligen Zeichenfolgen.

- Löschen von SSDs Nutzung von ATA Secure Erase oder Verschlüsselung und anschließendes Löschen des Schlüssels.

## Organisatorisches

- Verzeichnis der Bearbeitungstätigkeiten Dokumentation aller Aufbewahrungs- und Löschfristen.

- Prüfprozesse Regelmäßige Überprüfung der Einhaltung der Aufbewahrungsfristen und der Datensicherheit.

## Zusammenarbeit mit Dritten

- Vertragliche Bestimmungen Verträge mit Dienstleistern zur Aufbewahrung von Daten müssen Datenschutzanforderungen enthalten.

- Sicherheitsvorfälle Definition von Verfahren zur Behandlung von Sicherheitsvorfällen.

## Schulung und Sensibilisierung

- Alle Mitarbeiter sind regelmäßig über die Anforderungen dieser SOP zu schulen und für den Datenschutz zu sensibilisieren.

## Dokumentation und Kontrolle

- Dokumentation Alle Aufbewahrungs- und Löschvorgänge sind zu dokumentieren.

- Kontrolle Regelmäßige interne Audits zur Überprüfung der Einhaltung dieser SOP.

## Inkrafttreten

Diese SOP tritt mit sofortiger Wirkung in Kraft und ist regelmäßig zu überprüfen und bei Bedarf zu aktualisieren.