16.1. Datenschutz

Die RBSD sind verpflichtet, die Anforderungen zur Einhaltung des Datenschutzgesetzes umzusetzen.

16.2. Datensicherheit

16.2.1. Computergestützte Systeme

Wenn computergestützte Systeme eingesetzt werden, müssen Software, Hardware und Sicherungsverfahren regelmässig überprüft werden, um die Zuverlässigkeit zu gewährleisten.
Für kritische Systeme sollte eine aktuelle Systembeschreibung vorliegen, in der die physischen und logischen Datenflüsse und Schnittstellen zu anderen Systemen oder Prozessen, alle Hardware- und Software-Voraussetzungen sowie Sicherheitsmassnahmen definiert sind.

16.2.2. Validierungen und Testungen

Computergestützte Systeme müssen vor dem Einsatz mittels einem dokumentierten risikobasiertem Ansatz bewertet werden. Aufgrund dieser Bewertung müssen die Systeme gegebenenfalls validiert und im validierten Zustand gehalten werden.
Geeignete Testmethoden und Testszenarien sollten festgelegt und dokumentiert werden.
System-(Prozess-)Parametergrenzen, Datengrenzen und die Fehlerbehandlung sollen berücksichtigt werden. Die Bewertungen, Testungen, Angemessenheitsbeurteilung sind zu dokumentieren.
Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete eingebaute Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten enthalten, um die Risiken zu minimieren.
Integrität und Genauigkeit der Daten-Sicherung und die Fähigkeit, die Daten wiederherzustellen, sollten bei der Validierung überprüft und regelmäßig überwacht werden.
Relevante Änderungen in den computergestützten Systemen müssen vorgängig evaluiert und bewertet werden. Je nach Einstufung müssen diese validiert werden.

16.2.3. Massgeschneiderte -Kundenspezifische computergestützter Systeme

Für die Validierung massgeschneiderter oder kundenspezifischer computergestützter Systeme sollte ein Verfahren vorhanden sein, das die formale Bewertung und Berichterstattung über Qualitäts- und Leistungsmessungen für alle Lebenszyklusphasen des Systems gewährleistet.

16.2.4. Berechtigungen

Hardware und Software müssen gegen unbefugte Nutzung oder unbefugte Änderungen geschützt werden. Es sollte eine Hierarchie des erlaubten Benutzerzugangs zur Eingabe, Änderung, zum Lesen oder Drucken von Daten bestehen.

16.2.5. Risikomanagement

Das Risikomanagement sollte während des gesamten Lebenszyklus des computergestützten Systems angewandt werden, wobei die Spendersicherheit, die Patientensicherheit, die Datenintegrität und die Produktqualität berücksichtigt werden.
Der Benutzer sollte alle angemessenen Massnahmen ergreifen, um sicherzustellen, dass das System im Einklang mit einem geeigneten Qualitätsmanagementsystem entwickelt wurde. Der Lieferant sollte angemessen bewertet werden.
Es sollten alle erforderlichen Massnahmen getroffen werden, um den Schutz der Daten zu gewährleisten. Diese Massnahmen stellen sicher, dass Vorkehrungen gegen unbefugtes Hinzufügen, Übertragung von Informationen, Löschen oder Ändern von Daten getroffen werden, um Unstimmigkeiten in den Daten zu beseitigen und unbefugte Offenlegung solcher Informationen zu verhindern.

16.2.6. Datenintegrität

Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete eingebaute Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten enthalten, um die Risiken einer Fehlübermittlung zu minimieren.

Müssen Daten in einem anderen Format transferiert werden, muss sichergestellt werden, dass der ursprüngliche Wert und/ oder die Aussage während des Migrationsprozesses nicht verändert wird.

16.2.7. Manuelle Eingaben

Für kritische Daten, die manuell eingegeben werden, sollte eine zusätzliche Kontrolle der Richtigkeit der Daten erfolgen. Diese Überprüfung kann durch einen zweiten Mitarbeiter oder durch validierte elektronische Mittel erfolgen.
Die Kritikalität und die potenziellen Folgen von fehlerhaften oder falsch eingegebenen Daten für ein System, sollten durch ein Risikomanagement abgedeckt werden.

16.2.8. Wartungen / Updates

Die Systeme sollten jederzeit ordnungsgemäss gewartet sein. Wartungspläne für Computergestütze Systeme sollten wenn nötig erstellt und dokumentiert umgesetzt werden.

16.2.9. Back-up

Von allen relevanten Daten sollten regelmäßig Sicherungskopien erstellt werden.

16.2.10. Gewährleistung der Verfügbarkeit der Daten

Es sollten Vorkehrungen getroffen werden, um den Verlust und/oder die Beschädigung von Daten bei geplanter oder ungeplanter Downtime oder bei Funktionsstörungen des Computersystems zu verhindern.
Für computergestützte Systeme, die kritische Prozesse unterstützen, sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung für diese Prozesse im Falle eines Systemausfalls zu gewährleisten (z. B. ein manuelles oder alternatives System).
Die Zeit, die erforderlich ist, um die alternativen Vorkehrungen in Betrieb zu nehmen, sollte sich nach dem Risiko richten und für ein bestimmtes System und den von ihm unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten in angemessener Weise dokumentiert und getestet werden.

16.2.11. Dokumentation von Modifikationen

Bei Erstellung, Löschung oder Änderungen von Computeranwendungen sollte die Anwender-Dokumentation überarbeitet werden und das zuständige Personal entsprechend geschult werden, bevor eine Änderung in den Routinebetrieb übernommen wird. Eingesetzte Benutzertests sollen nachweisen, dass das System allen Anforderungen entspricht, sowohl bei der Erstinstallation als auch nach jeder Systemänderung.

16.2.12. Archivierung der Daten

Daten die aufgrund gesetzlicher Vorgaben archiviert werden müssen, sollten gegen Beschädigung und Verlust gesichert werden. Archivierte Daten sollten auf ihre Zugänglichkeit, Lesbarkeit, Richtigkeit und Vollständigkeit überprüft werden. Der Zugang zu den Daten sollte während des gesamten Archivierungszeitraums gewährleistet sein.
Wenn relevante Änderungen am System vorgenommen werden (z. B. Computerausrüstung oder Programme), sollte die Möglichkeit des Abrufs der Daten sichergestellt und getestet werden.
Weiter sind die Berechtigungen wie z.B. für das Löschen oder Vernichten von Daten zu definieren.

16.2.13. Freigabe relevante Computersysteme

Computersysteme, die für die Kontrolle von Entscheidungen im Zusammenhang mit Beständen und der Freigabe von Blutbestandteilen ausgelegt sind, sollten die Freigabe von Blut oder Blutbestandteilen, die als nicht zur Freigabe geeignet

gelten, verhindern. Es sollten Mechanismen vorhanden sein, die die Gewinnung und Freigabe von Bestandteilen einer künftigen Spende eines kontraindizierten Spenders verhindern.