BLUTSPENDE SRK SCHWEIZ
TRANSFUSION CRS SUISSE
TRASFUSIONE CRS SVIZZERA

Seitenhistorie

Freigegeben ("**Gültig**" anzeigen)

Versionen im Vergleich

7	Aktuell
Sandra Kurth	Tiziana Janner
12.11.2024	15.05.2025

Schlüssel

Diese Zeile wurde hinzugefügt.
~~Diese Zeile wurde entfernt.~~
Formatierung wurde geändert.

Seitenhistorie anzeigen

Majorversion:
2
Minorversion:
2.0
Dokumentennummer:
3507

...

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

Datensicherheit

~~**GPG relevante Änderungen**~~ ~~**(Weiss nicht genau wohin dieser Abschnitt gehört)**~~

~~Auf der Grundlage einer Risikobewertung sollte in Erwägung gezogen werden, in das System Folgendes einzubauen:~~

- ~~Die Aufzeichnung GPG-relevanten Änderungen und Löschungen (ein vom System generierter "Prüfpfad").~~
- ~~Für eine Änderung oder Löschung von GPG-relevanten Daten sollte der Grund dokumentiert werden.~~
- ~~Audit Trails müssen in allgemein verständlicher Form verfügbar und umsetzbar sein und regelmäßig überprüft werden.~~

Computergestützte Systeme

...

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. ~~Es sollte eine Hierarchie des erlaubten Benutzerzugangs zur Eingabe, Änderung, zum Lesen oder Drucken von Daten bestehen.~~

Massgeschneiderte -Kundenspezifische computergestützter Systeme

...

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 .

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.

Datenintegrität

~~Das Sicherungsverfahren muss den Verlust oder die Beschädigung von Daten bei erwarteten und unerwarteten Ausfallzeiten oder Funktionsstörungen verhindern.~~
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.

...

Von allen relevanten Daten sollten regelmäßig Sicherungskopien erstellt werden.