Articolo 16 Protezione dei dati/sicurezza dei dati

Tipo di documento: ART
Versione: 2
Valido da: 01.07.2025

Nuovo articolo

16.1. Protezione dei dati

Il STR è tenuto a soddisfare i requisiti per il rispetto della legge sulla protezione dei dati.

16.2. Sicurezza dei dati

16.2.1. **Sistemi informatici**

Quando si utilizzano sistemi informatici, è necessario controllare regolarmente il software, l'hardware e le procedure di sicurezza per garantirne l'affidabilità.

Per i sistemi critici dovrebbe essere disponibile una descrizione aggiornata del sistema che definisca i flussi di dati fisici e logici e le interfacce con altri sistemi o processi, tutti i requisiti hardware e software e le misure di sicurezza.

16.2.2. **Convalida e test**

I sistemi informatici devono essere valutati prima dell'uso con un approccio documentato basato sul rischio. Sulla base di tale valutazione, i sistemi devono essere convalidati, se necessario, e mantenuti in uno stato convalidato. È necessario definire e documentare metodi di prova e scenari di test adeguati. È necessario tenere conto dei limiti dei parametri di sistema (di processo), dei limiti dei dati e della gestione degli errori. Le valutazioni, i test e la valutazione dell'adeguatezza devono essere documentati. I sistemi informatici che scambiano dati elettronicamente con altri sistemi devono disporre di controlli integrati adeguati per garantire l'immissione e l'elaborazione corretta e sicura dei dati, al fine di ridurre al minimo i rischi. L'integrità e l'accuratezza della protezione dei dati e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate regolarmente. Le modifiche rilevanti nei sistemi informatizzati devono essere preventivamente valutate e analizzate. A seconda della classificazione, devono essere convalidate.

16.2.3. **Sistemi informatici personalizzati e specifici per il cliente**

Per la convalida di sistemi informatici personalizzati o specifici per il cliente dovrebbe essere disponibile una procedura che garantisca la valutazione formale e la rendicontazione delle misurazioni della qualità e delle prestazioni per tutte le fasi del ciclo di vita del sistema.

16.2.4. **Autorizzazioni**

L'hardware e il software devono essere protetti contro l'uso non autorizzato o modifiche non autorizzate. Deve esistere una gerarchia di accesso degli utenti autorizzati all'inserimento, alla modifica, alla lettura o alla stampa dei dati.

16.2.5. **Gestione del rischio**

La gestione dei rischi dovrebbe essere applicata durante l'intero ciclo di vita del sistema informatizzato, tenendo conto della sicurezza dei donatori, della sicurezza dei pazienti, dell'integrità dei dati e della qualità del prodotto.

L'utente dovrebbe adottare tutte le misure adeguate per garantire che il sistema sia stato sviluppato in conformità con un sistema di gestione della qualità adeguato. Il fornitore dovrebbe essere valutato in modo adeguato.

Dovrebbero essere prese tutte le misure necessarie per garantire la protezione dei dati. Tali misure garantiscono che siano prese precauzioni contro l'aggiunta, il trasferimento, la cancellazione o la modifica non autorizzati di informazioni, al fine di eliminare incongruenze nei dati e impedire la divulgazione non autorizzata di tali informazioni.

16.2.6. **Integrità dei dati**

I sistemi informatici che scambiano dati elettronicamente con altri sistemi dovrebbero disporre di controlli integrati adeguati per garantire l'immissione e il trattamento corretti e sicuri dei dati, al fine di ridurre al minimo i rischi di errori di trasmissione.

Se i dati devono essere trasferiti in un altro formato, è necessario garantire che il valore e/o il significato originario non venga alterato durante il processo di migrazione.

16.2.7. **Inserimenti manuali**

Per i dati critici inseriti manualmente è necessario effettuare un ulteriore controllo dell'esattezza dei dati. Tale verifica può essere effettuata da un secondo collaboratore o tramite strumenti elettronici convalidati.

La criticità e le potenziali conseguenze di dati errati o inseriti in modo errato per un sistema devono essere coperte da una gestione dei rischi.

16.2.8. **Manutenzione / Aggiornamenti**

I sistemi devono essere sottoposti a regolare manutenzione. Se necessario, occorre redigere piani di manutenzione per i sistemi informatici e documentarne l'attuazione.

16.2.9. **Backup**

È necessario eseguire regolarmente copie di backup di tutti i dati rilevanti.

16.2.10. **Garanzia della disponibilità dei dati**

È necessario adottare misure preventive per evitare la perdita e/o il danneggiamento dei dati in caso di interruzioni programmate o non programmate o di malfunzionamenti del sistema informatico.

Per i sistemi informatici che supportano processi critici, è necessario adottare misure preventive per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo).

Il tempo necessario per attivare le misure alternative dovrebbe essere basato sul rischio e adeguato al sistema specifico e al processo aziendale da esso supportato. Tali misure dovrebbero essere adeguatamente documentate e testate.

16.2.11. **Documentazione di modifiche**

In caso di realizzazione, cancellazione o modifica di applicazioni informatiche, è necessario rivedere la documentazione per gli utenti e formare adeguatamente il personale responsabile prima di introdurre qualsiasi cambiamento nelle operazioni di routine. I test utente effettuati devono dimostrare che il sistema soddisfa tutti i requisiti, sia al momento della prima installazione che dopo ogni modifica del sistema.

16.2.12. **Archiviazione dei dati**

I dati che devono essere archiviati in base alle disposizioni di legge devono essere protetti da danni e perdita. I dati archiviati devono essere verificati per quanto riguarda l'accessibilità, la leggibilità, la correttezza e la completezza. L'accesso ai dati deve essere garantito per tutto il periodo di archiviazione.

Se vengono apportate modifiche rilevanti al sistema (ad es. apparecchiature informatiche o programmi), è necessario garantire e verificare la possibilità di recuperare i dati.

È inoltre necessario definire le autorizzazioni, ad esempio per la cancellazione o la distruzione dei dati.

16.2.13. Autorizzazione dei sistemi informatici rilevanti

I sistemi informatici progettati per controllare le decisioni relative alle scorte e alla liberazione dei componenti del sangue devono impedire la liberazione di sangue o di componenti del sangue ritenuti non idonei alla liberazione. Devono essere previsti meccanismi che impediscano il prelievo e la liberazione di componenti di una futura donazione di un donatore controindicato.