Buone Pratiche di Fabbricazione in ambito farmaceutico - EU GMP - Revisione Annex 11 2011: La Gestione dei Sistemi Computerizzati - EU Legislation - EudraLex - The Rules Governing Medicinal Products in the European Union Volume 4 -Guidelines for good manufacturing practices for medicinal products for human and veterinary use - Good Manufacturing Practice - Medicinal Products for Human and Veterinary Use - Annex 11: Computerised Systems

Buone Pratiche di Fabbricazione Europee in ambito farmaceutico
La revisione dell'Annex 11: La Gestione dei Sistemi Computerizzati

"EudraLex - The Rules Governing Medicinal Products in the European Union - Volume 4 - Good Manufacturing Practice - Medicinal Products for Human and Veterinary Use - Annex 11: Computerised Systems"

L'allegato numero 11 (Annex 11) al Volume 4 delle EU-GMP tratta la Gestione dei Sistemi Informatici, operanti in ambiti regolamentati dalle Buone Pratiche di Fabbricazione. L'Agenzia Europea del Farmaco ha revisionato l'Annex 11 in risposta alla maggiore diffusione e complessità dei Sistemi Informatici, il documento è in vigore a partire dal 30 giugno 2011.
L'Annex 11 richiede che, i sistemi informatici operanti in ambiti regolamentati, siano Convalidati e l'Infrastruttura IT sia Qualificata.
Nei casi in cui un Sistema Computerizzato sostituisca un funzionamento manuale, deve essere garantito che non si verifichi una diminuzione della Qualità dei Prodotti, Controllo di Processo o Assicurazione della Qualità.
Deve essere provato che non sia presente alcun aumento del Rischio sul processo funzionale che gestisce il Sistema Informatico.

La *Gestione del Rischio* (*Risk Management*) deve essere applicata a tutto il *Ciclo di Vita* del Sistema Informatico, considerando:

- la Sicurezza dei Pazienti,
- l'Integrità dei Dati,
- la Qualità del Prodotto.

Le decisioni sulla portata delle attività di Validazione e dei controlli sulla Integrità dei Dati, devono basarsi su un'attività di *Valutazione del Rischio del Sistema Informatico* che evidenzi, il giustificativo delle decisioni intraprese. Tali valutazioni devono essere considerate come parte integrante del *Sistema di Gestione del Rischio*.

Tutto il Personale coinvolto nelle attività del Sistema Informatico (Process Owner, System Owner, Qualified Persons, IT e Utenti) deve possedere adeguata *Qualifica, Livello di Accesso e Responsabilità* al fine di poter svolgere i compiti loro assegnati.

Quando *Terze Parti,* ad esempio fornitori di sistemi o servizi, vengono utilizzati per :

- Fornire,
- Installare,
- Configurare,
- Integrare,
- Validare,
- Manutenere (ad esempio tramite accesso remoto),
- Modificare;

un Sistema Informatico oppure un servizio collegato oppure svolgere una elaborazione dei dati, tra il Cliente e le Terze Parti, devono esistere accordi formali (*Service Level Agreement*, *Quality Agreement* o *Technical Agreement*) . Tali accordi devono includere chiaramente quali siano le Responsabilità delle Terze Parti.
Il *Reparto IT* aziendale deve essere considerato analogamente ad una Terza Parte, per la fornitura dei suoi servizi.

La competenza e l'affidabilità di un fornitore sono i fattori chiave nella scelta di un prodotto o fornitore di servizi. La necessità di un *Audit* deve essere basata su una Valutazione dei Rischi della data fornitura.

La documentazione fornita con i prodotti disponibili commercialmente (off-the-shelf), deve essere revisionata da parte degli utenti per riscontrare che siano soddisfatti tutti i Requisiti Utente (*User Requirement Specifications*).

Il Sistema Qualità e le informazioni sugli Audit, relativi ai fornitori o a sviluppatori di software/sistemi devono essere messi a disposizione degli Ispettori in caso di loro richiesta.

La *Documentazione di Convalida* e i relativi Report devono coprire i passi più importanti del Ciclo di Vita del Sistema. L'Azienda Farmaceutica deve essere in grado di giustificare i propri:

- Standard,
- Protocolli,
- Criteri di Accettazione,
- Procedure,
- Registrazioni;

in base alla relativa Valutazione del Rischio.

La *Documentazione di Convalida* deve comprendere:

- la Documentazione di Gestione delle Modifiche (se applicabile)
- i Report su eventuali scostamenti che si siano verificati durante il Processo di Convalida.

Deve essere disponibile ed aggiornato, l'Inventario dei Sistemi Computerizzati rilevanti ed il dettaglio della loro funzionalità ad impatto GMP.

Per i *Sistemi Critici* deve essere disponibile una descrizione, aggiornata e dettagliata, di sistema, comprendente:

- le Modalità Funzionali fisiche e logiche,
- il Flusso Dati con altri sistemi o processi,
- le Interfacce con altri sistemi o processi,
- i Requisiti Hardware e Software,
- le Misure di Sicurezza.

La documentazione di Specifiche (*Functional Specifications*) deve dettagliare le funzioni del Sistema Computerizzato e deve basarsi sulla Valutazione del Rischio e sull'impatto GMP.
Le Specifiche di Sistema definite, devono avere completa tracciabilità per tutto il Ciclo di Vita del Sistema.

L'Utente deve adottare tutte le misure ragionevoli per assicurare che il sistema sia stato sviluppato in conformità ad un adeguato Sistema di Gestione della Qualità.

In caso di Convalida di Sistemi Personalizzati (Bespoke/Customized computerised system), deve essere definito un processo che assicuri la valutazione formale della qualità e delle prestazioni per tutte le fasi del Ciclo di Vita del Sistema.

Una adeguata documentazione sui collaudi funzionali deve essere redatta. In particolare, devono essere considerati:

- i parametri limiti di sistema/processo,
- i valori limite dei dati,
- la gestione degli errori.

Modalità di testing automatico e comunque l'utilizzo di ambienti di test, devono essere valutati per la loro adeguatezza.

Se i dati vengono trasferiti in un altro sistema oppure convertiti in un altro formato, la validazione deve includere i controlli che verifichino che i dati non siano stati modificati in valore e/o significato, nel corso del *Processo di Migrazione* o *Conversione*.

Nel caso di Sistemi Informatici che scambiano dati con altri Sistemi, devono essere considerati opportuni controlli, affinché tale attività avvenga in modo sicuro, con riduzione al minimo dei rischi di fallimento.

Per i *dati critici*, inseriti manualmente, deve essere considerato un ulteriore controllo sulla correttezza dei dati inseriti. Questa verifica può essere effettuata da un secondo operatore o da Sistemi Informatici convalidati.
Le criticità e le potenziali conseguenze, di un erroneo o non corretto inserimento dati in un Sistema, devono essere valutate dalla Gestione del Rischio.

I *dati elettronici* devono essere garantiti, da mezzi sia fisici che elettronici, contro i danni. I dati archiviati devono essere controllati in modo che garantiscano la loro accessibilità, leggibilità e accuratezza.
L'accesso ai dati deve essere garantito per tutto il loro periodo di mantenimento.

Regolari *Back-up* dei dati critici devono essere eseguiti. L'integrità e la precisione dei backup dati e la possibilità di ripristinare i dati, devono essere controllati durante la convalida e monitorati periodicamente.

Deve essere possibile ottenere *copie stampate*, accurate, dei dati memorizzati elettronicamente.
Per i record a sostegno del *Rilascio dei Lotti*, deve essere possibile generare stampe che indichino se uno dei dati è stato modificato dopo l'inserimento dei dati originari.

Occorre considerare, sulla base di una Valutazione dei Rischi, la disponibilità, nel Sistema, di un registro contenente tutte le modifiche a rilevanza GMP ("*Audit Trail*" di Sistema). Per la modifica o cancellazione dei dati a rilevanza GMP deve essere documentate la motivazione di tale attività.
Gli Audit Trails devono essere disponibili in una forma comprensibile e regolarmente revisionati.

Eventuali modifiche ad un Sistema Computerizzato, che comprendano anche le configurazioni di sistema, devono poter essere effettuate solo in modo controllato, secondo una Procedura definita.

I Sistemi Informatici devono essere *periodicamente revisionati,* per confermare la loro permanenza in stato convalidato e la loro conformità alle GMP, tale attività deve essere regolata da procedura dedicata.
Tali valutazioni devono includere, se applicabili:

- l'attuale gamma di funzionalità,
- i record di deviazione,
- gli incidenti,
- i problemi,
- la storia degli aggiornamenti,
- le prestazioni,
- l'affidabilità,
- la sicurezza,
- i report sullo stato di convalida.

Controlli sulla Sicurezza fisica e/o logico devono essere messi in atto per limitare l'accesso informatico alle persone autorizzate.
Metodi adatti per prevenire l'accesso non autorizzato al Sistema potrebbero includere:

- l'uso di chiavi,
- l'uso di badge,
- codici personali con password,
- l'uso di accessi biometrici,
- limitazioni di accesso fisico alle attrezzature informatiche e/o aree di elaborazione dati.

L'estensione dei controlli di sicurezza dipende dalla criticità del sistema informatico.

La Creazione, Modifica e Revoca di autorizzazioni di accesso deve essere registrata.
Sistemi di Gestione per i Dati e per i Documenti devono essere progettati per registrare le identità degli operatori che entrano, modificano, confermano o eliminano dei dati, comprendendo anche data e ora dell'attività svolta.

Tutti gli *Incidenti*, non solo errori di sistema e/o errori di dati, devono essere segnalati e valutati. La causa principale di un evento critico deve essere individuata e devono definite le *Azioni Correttive e Preventive*.

I *Record Elettronici* possono essere firmati elettronicamente.
La *firma elettronica* deve essere preveista in modo tale che:

- abbia lo stesso impatto delle firme autografe all'interno della società,
- sia permanentemente legata al rispettivo record,
- comprenda l'ora e la data.

Quando un Sistema Informatizzato viene utilizzato per la registrazione della certificazione e del rilascio del lotto; il sistema deve permettere solo alle *Qualified Person* di certificare il rilascio dei lotti. Il sistema deve, chiaramente, identificare e registrare la persona che rilascia o certifica i lotti.
L'attività deve essere effettuata mediante una firma elettronica.

Affinché sia garantita la continuità delle attività critiche di carattere business, si devono valutare metodi alternativi in caso di un fallimento del Sistema Computerizzato (ad esempio attività manuali o sistemi alternativi).
Il tempo necessario per portare in operativo la modalità alternativa, deve essere basato sul rischio e dimensionato per il particolare sistema e processo che definisce. Tali disposizioni devono essere adeguatamente documentate e testate.

I dati possono essere *archiviati*. Questi dati devono essere controllati per accessibilità, leggibilità e integrità. In caso di modifiche rilevanti a carico del sistema (ad esempio componenti hardware o software), la possibilità di recuperare i dati deve essere garantita e testata.

28 Settembre 2012 (ultimo aggiornamento)

Studio di Ingegneria Ing.Andrea Giampellegrini - Via Fucini, 35 - 56127 Pisa - Email : info@ingag.it
C.F. GMPNDR74A21G337U - P.IVA 01950000503