QUADERNO

"PHARMA 4.0: OPPORTUNITÀ E VINCOLI DELLA DIGITALIZZAZIONE DELL'INDUSTRIA FARMACEUTICA"

"PHARMA 4.0: OPPORTUNITIES AND CONSTRAINTS OF THE PHARMACEUTICAL INDUSTRY DIGITALIZATION"

Come assicurare la conformità delle soluzioni Industry 4.0 ai requisiti delle GMP e della data integrity

How to ensure compliance of Industry 4.0 solutions with GMP requirements and data integrity

Pier Luigi Agazzi

GAMP Italia, Lomazzo (CO)

La Industry 4.0 ha dato nuovo impulso all'introduzione di sistemi informatici integrati anche in ambiti regolati. Tali sistemi sono soggetti ai requisiti regolatori delle buone pratiche di fabbricazione (GMP) e in particolare della convalida dei sistemi e dell'integrità dei dati (*data integrity*). Ovvero, se il sistema svolge funzioni a impatto diretto/indiretto sulla qualità del prodotto occorre dimostrare e documentare il "buon funzionamento", incluse le persone che li utilizzano (la convalida del sistema). Se poi il sistema memorizza dati elettronici occorre assicurare che i dati elettronici siano sicuri e possano essere usati in sostituzione della carta (la data integrity). Per la convalida dei sistemi viene esaminata la linea guida GAMP 5 che propone i concetti di base del ciclo di vita del software, delle categorie del software e dell'analisi dei rischi, per pianificare ed eseguire le attività di convalida dei sistemi, come richiesto dalle GMP. È poi stata utilizzata la linea guida GAMP sulla data integrity per illustrare i concetti fondamentali della governance dei dati, che a partire dalle definizioni del ciclo di vita dei dati (dati grezzi, metadati, ecc.) e dei requisiti della data integrity (ALCOA) portano alle misure da implementare sui sistemi per assicurarne la integrità. In particolare per i dati in formato elettronico: accessi controllati, backup e restore, inalterabilità di data e ora ecc. Ci auguriamo che queste linee guida agevolino l'introduzione dei sistemi di Industry 4.0 nell'industria farmaceutica italiana, consentendole di rimanere all'avanguardia in questo settore così importante.

Parole chiave: Industry 4.0, integrità dei dati

The Industry 4.0 program is giving a new incentive to the introduction of integrated computerized systems also in regulated industry sectors. These systems are subject to Good Manufacturing Practice (GMP) regulatory requirements and in particular to the validation and the data integrity requirements. Therefore, if the system performs functionalities with direct/ indirect impact on the product quality (or patient health), it is necessary to validate the system. This consist of the demonstration and documentation of the "proper functionality" of the system, including the proper use by the system users. Further, if the system stores GMP data in electronic format, it is necessary to ensure that they are secure, then they can be used in substitution of paper records (data integrity). For the validation of computerized systems the article summarized, the content of the GAMP 5 guideline that propose the concepts of: software development life cycle, software categories and Risk Analysis to plan and execute the computerized systems validation activities, as required by the GMP. The GAMP "Records and Data Integrity Guide" is then discussed, in order to explain the basic concepts of a Data governance that, starting from the definitions of the Data Life Cycle (raw data, metadata etc.) and of the data integrity requirements (ALCOA), leads to the measures to be implemented on the computerized systems in order to ensure the data integrity. That is, in particular for data in electronic format: controlled accesses, backup and restore, date and time inalterability etc.

Address for correspondence
Indirizzo per la corrispondenza

Pier Luigi Agazzi
Adeodata S.r.l
c/o ComoNext,
via Cavour 2, 22074 Lomazzo (CO)
e-mail: pierluigi.agazzi@adeodata.eu

We hope that these guidelines will facilitate the introduction of Industry 4.0 systems into the Italian pharmaceutical industry, allowing it to remain at the forefront of this important sector.

Key words: *Industry 4.0, data integrity*

Glossario

LIMS: *Laboratory Information Management System*
SCADA: *Supervision Control and Data Acquisition*
DCS: *Distributed Control System*
ERP: *Enterprise Resources Planning*
ADR: *Adverse Events Reporting System*
CDS: *Chromatographic Data System*
EDMS: *Electronic Document Management System*
CRM: *Customer Relationship Management System*
CQA: Indicatori critici della qualità del prodotto
CPP: Parametri critici del processo

Introduzione

La Industry 4.0 ha dato nuovo impulso all'introduzione di sistemi informatici in ambiti regolati.

Tali sistemi sono soggetti ai requisiti regolatori delle buone pratiche di fabbricazione (GMP) e in particolare della convalida dei sistemi e dell'integrità dei dati (*data integrity*).

Ovvero, se il sistema svolge funzioni a impatto diretto/indiretto sulla qualità del prodotto occorre assicurarne il "buon funzionamento", incluse le persone che li utilizzano, (la convalida del sistema).

Se poi il sistema memorizza dati elettronici occorre assicurare che i dati elettronici siano sicuri e possano essere usati in sostituzione della carta (la data integrity).

In questo articolo vengono presentati i concetti fondamentali della convalida dei sistemi e della *Data Integrity* secondo le linee guida GAMP, attualmente le più diffuse sul mercato.

La convalida dei sistemi (le GAMP 5)

Le linee guida GAMP per la convalida dei sistemi computerizzati (*Good Automated Manufacturing Practice*), dopo la prima versione del lontano 1994, sono arrivate alla versione 5 pubblicata nel 2008 (GAMP 5, 2008).

Le linee guida sono da intendersi come una semplice interpretazione dei requisiti normativi, come un suggerimento su come questi possano essere soddisfatti, non sono quindi obbligatorie. Sono però molto utili per allineare le attività di convalida dei sistemi computerizzati tra le varie industrie, gli enti regolatori e i fornitori di sistemi.

Il documento è strutturato in due parti principali, la prima fornisce una presentazione dei concetti fondamentali per la convalida: il ciclo di vita del software, le categorie del software (e dell'hardware) e la risk analysis (Fig. 1).

Nelle appendici (la seconda parte) vengono riportate numerose procedure per la redazione dei documenti che costituiscono un prezioso ausilio nella convalida di questi sistemi.

Le appendici sono organizzate in 3 gruppi:

- management;
- development;
- operation.

Nella prima parte viene richiamata la definizione della convalida data dalla FDA nel 1987: "dare un'evidenza documentata che assicuri con un elevato grado di certezza che uno specifico processo produca un prodotto finale conforme ai requisiti di qualità prestabiliti" (*Food and Drug Administration*, 1987). Poi vengono presentati i concetti fondamentali delle GAMP descritti nel seguito.

Il ciclo di vita del software

Il principio alla base della convalida è che un sistema sia stato progettato e realizzato secondo un sistema di qualità che a partire dalla documentazione di progetto iniziale porti alle verifiche di identificazione del sistema e delle sue prove funzionali formalizzate in adeguati documenti di test, una volta denominati protocolli di *Installation Qualification* (IQ), *Operational Qualification* (OQ) e *Performance Qualification* (PQ).

L'iter di sviluppo del sistema computerizzato originariamente denominato "ciclo di sviluppo" del software (a V o a cascata), ora è stato esteso a coprire anche la fase iniziale di studio di fattibilità, e le fasi successive di utilizzo ed eventuale dismissione per formare il "ciclo di vita" del software è rappresentato in Figura 2.

Il ciclo di vita dovrebbe essere incluso nel sistema qualità del fornitore, che dovrebbe essere oggetto di audit da parte del cliente finale. Come nel caso di tutte le attività critiche

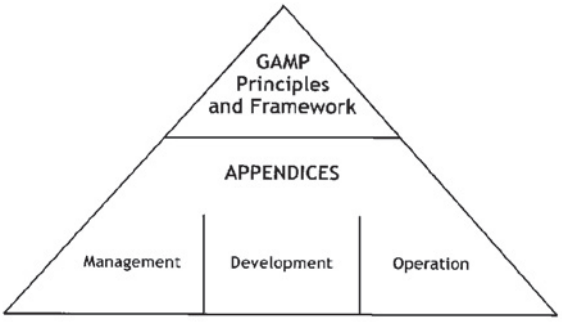

Figura 1.
Struttura delle linee guida GAMP.

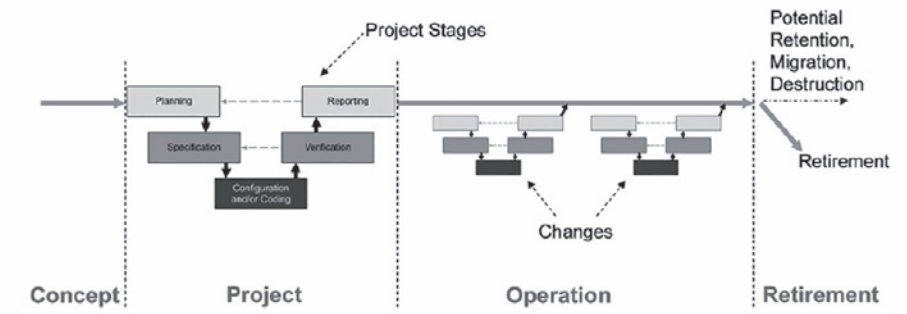

Figura 2.
Approccio alla risk analysis.

affidate a terzi, l'audit dovrebbe costituire la base per la scelta del fornitore. Lo scopo è quello di verificare i seguenti punti:
- capacità tecnica del fornitore;
- capacità di soddisfare i requisiti della convalida;
- sistemi di assicurazione della qualità e di controllo delle attività di sviluppo.

Strategie di convalida delle diverse tipologie del software

Dato che esistono sul mercato software di diversa complessità, per focalizzare le attività di convalida sulle funzioni più utilizzate e meno collaudate, viene individuato il livello dove il software viene adattato alla applicazione e proprio su questi aspetti applicativi si concentra lo sforzo di convalida, come riassunto nella seguente tabella che a sinistra indica le "categorie del software" e per ciascuna di esse, nella colonna di destra indica quali sono le attività di convalida considerate minime richieste:

1 i software d'infrastruttura, come i sistemi operativi: sono disponibili commercialmente, non sono soggetti a qualifiche o test specifici, ma occorre tenerne sotto controllo la versione, gli eventuali aggiornamenti (inclusi i service pèack) o eventuali aggiornamenti dell'hardware;
2 firmware: con la versione 5 delle GAMP non viene più utilizzata. Possono però avere anche dei parametri con cui è possibile affinarne il funzionamento, pertanto anche la configurazione di questi parametri va registrata in fase di qualifica dell'installazione;
3 i pacchetti software non configurati: sono i software standard disponibili in commercio che svolgono determinate funzioni e che per funzionare richiedono solo l'inserimento dei dati specifici dell'utente. In questa categoria sono stati inclusi software che sarebbero configurabili, ma che sono stati installati nella configurazione di default (standard). Oltre alle precauzioni da usare per i sistemi operativi viene richiesta la convalida delle funzioni utilizzate, ovvero quelle indicate nei requisiti utente e in particolare di:
   - algoritmi e parametri critici;
   - integrità, precisione e affidabilità dei dati;
   - procedure operative.
4 i pacchetti software configurati: sono ad esempio i sistemi di controllo e supervisione (DCS o SCADA) i sistemi di gestione dei laboratori (LIMS) e i sistemi gestionali (ERP). Per questi sistemi l'utente configura alcune funzioni (ad esempio prelevandole da una libreria o modificandone alcuni parametri operativi) per adattarle alle esigenze della sua applicazione, senza però modificarne il codice sorgente. Oltre alle precauzioni indicate per i sistemi di cui al punto precedente è necessaria la verifica della configurazione e si raccomanda un'attività di qualifica dei fornitori (audit);
5 i software (o parti di software) sviluppati appositamente per un'applicazione. Sono i software il cui sviluppo deve seguire il ciclo completo della convalida del software, inclusi i test interni del fornitore, che possono essere verificati tramite l'Audit al fornitore (Tab. I).

Come esempio possiamo considerare i fogli elettronici (cui è dedicata una appendice specifica delle GAMP) che vengono inseriti nella categoria:
- 1 se utilizzati solo per stampare dati;
- 3/4 se usati con formule (secondo la complessità dei calcoli);
- 5 se si utilizzano delle macro.

Una significativa novità delle GAMP 5 è stata l'introduzione di due ulteriori criteri per la determinazione dell'entità delle attività di convalida:
- il grado di novità del sistema: un sistema appena introdotto sul mercato verosimilmente presenterà un maggior numero di anomalie di un sistema ormai maturo; questo dovrebbe riflettersi in un maggior numero di test;
- i risultati dell'audit al fornitore: se si riscontrano delle carenze nel sistema qualità del fornitore, ad esempio in termini di test interno o di documentazione, durante la convalida occorrerà sopperire a queste carenze.

Risk analysis

L'assunzione di base delle attuali GMP è che il rigore delle attività di convalida dovrebbe essere commisurato alla criticità delle funzioni di un sistema.

In linea con l'ICH Q9 (ICH, 2005) e lo standard

Tabella I.

Categoria	*Tipo di software*	*Esempio*	*Strategia di convalida*
1	Software di infrastruttura	Sistemi operativi, database, middleware, compilatori di programmi, software statistici, fogli elettronici, software di sorveglianza della rete, software di controllo delle versioni ecc.	Registrazione della versione
2	Firmware	Non più utilizzata	
3	Software non configurati	Applicazioni basate su firmware, software commerciali, strumenti	Test dei requisiti
4	Software configurati (adattati con parametri al processo del cliente)	LIMS, SCADA, DCS, ERP, *Clinical Trial Monitoring*, ADR *Reporting*, CDS, EDMS, *Building Management Systems*, CRM, Fogli elettronici	Verifica della configurazione + Test dei requisiti
5	Software personalizzati (con codice sviluppato apposta per il cliente)	Applicazioni sviluppate internamente o esternamente: PLC, *Custom Software*, Fogli elettronici (con macro)	Test dei singoli moduli + test di integrazione + test dei requisiti

ISO 14971 (ISO, 2000), le GAMP 5 propongono l'approccio alla risk analysis in 5 step, come illustrato in Figura 3.

Il punto di partenza è la conoscenza scientifica del prodotto (con i sui *Critical Quality*, CQA), del processo (con i suoi *Critical Process Parameters*, CPP) e di come questi possono essere influenzati dal sistema computerizzato che li controlla e li gestisce.

Sulla base di questa conoscenza diviene possibile identificare potenziali scenari in cui il fallimento del sistema di soddisfare i requisiti attesi può generare rischi inaccettabili per il

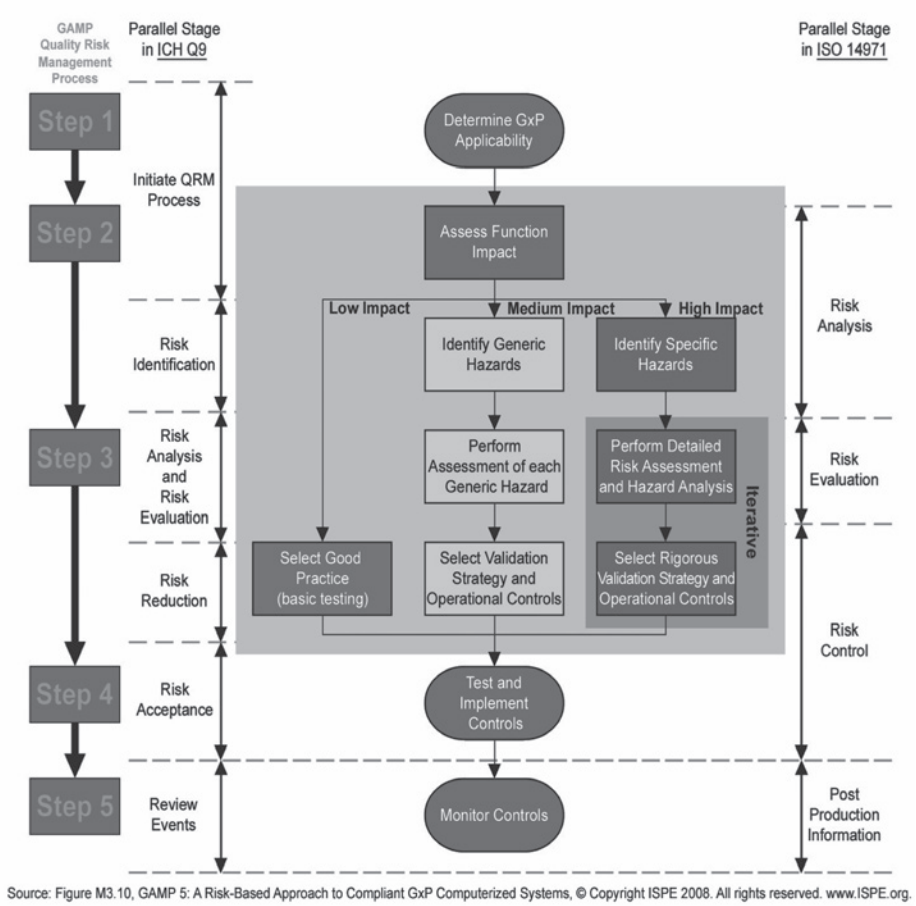

Figura 3.
Parallelo tra fasi della risk analysis delle GAMP 5, ICH Q9 e ISO 14971.

prodotto e/o i pazienti. Il citato Q9 indica il rischio come la combinazione di tre fattori:

- l'impatto sulla qualità del prodotto o la salute del paziente;
- la probabilità dello scenario di rischio;
- la rilevabilità dello scenario di rischio.

Viene dapprima valutata l'applicabilità delle GxP (step 1). Poi (step 2) viene valutato il potenziale impatto di una funzione e (step 3) in caso di impatto:

- basso, ci si limita ad applicare delle buone pratiche di ingegneria;
- medio, viene valutata la probabilità e la rilevabilità di un malfunzionamento generico della funzione;
- elevato, vengono esaminati diversi scenari di rischio e per ciascuno viene valutata la probabilità e la rilevabilità.

Una volta identificati gli scenari di rischio è possibile valutare la possibilità di mitigare il rischio con degli adeguati controlli, come ad esempio individuare condizioni di errore e indicare adeguate misure correttive.

Un altro strumento per la mitigazione del rischio è costituito da un maggiore livello di testing delle funzioni critiche, per aumentare la confidenza nell'affidabilità del sistema nelle diverse condizioni operative.

I controlli dovranno poi essere implementati e testati (convalidati) (step 4).

Infine l'efficacia di questi controlli andrà sorvegliata nel tempo, durante il periodo di utilizzo del sistema (step 5).

Pur proponendo il suo approccio, le GAMP 5 non escludono l'utilizzo di altri standard per la risk analysis.

La data integrity

Come detto, se un sistema computerizzato memorizza dati elettronici occorre assicurarne l'integrità, cioè che siano sicuri e possano essere usati in sostituzione della carta.

Anche qui faremo riferimento a una linea guida GAMP: "*Records and Data Integrity Guide*" (ISPE©GAMP, 2017).

La linea guida si focalizza sulla governance della data integrity, di cui un'azienda regolata si deve dotare, ovvero: "Il complesso delle misure messe in atto per assicurare che il dato, indipendentemente dal formato in cui viene generato (elettronico o cartaceo), venga registrato, elaborato, conservato e utilizzato in modo da assicurarne l'integrità (ovvero la completezza, consistenza e accuratezza) per tutto il suo ciclo di vita".

Nel seguito vengono descritti i contenuti fondamentali di questa governance.

Il ciclo di vita dei dati

Il ciclo di vita dei dati è il percorso dei dati dalla loro generazione alla loro dismissione, passando per il loro utilizzo.

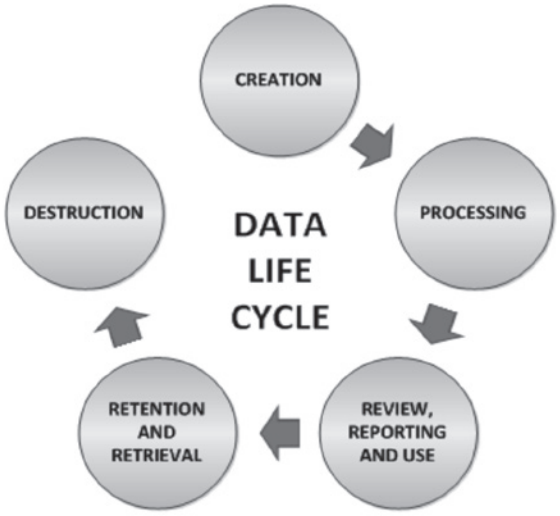

Figura 4.
Ciclo di vita del dato.

Un'illustrazione di questo ciclo è riportata in Figura 4. Si tratta di un caso semplificato in quanto i dati possono seguire percorsi più complessi, essere importati, esportati, aggregati, migrati ecc.

Il ciclo è comunque utile per comprendere i seguenti termini utilizzati per la data integrity:

- dati originali (dati grezzi o "raw data"): sono i dati nella forma in cui sono stati generati *(creation)*, come osservazioni manuali scritte su carta o dati acquisiti automaticamente in formato elettronico.

I dati grezzi devono essere immediatamente e accuratamente registrati. Essi vengono usati per generare altri dati o registrazioni, quindi vanno conservati in modo da permettere la ricostruzione dei dati da essi derivati;

- dati: sono informazioni derivate o ottenute dai record originali (*processing*), come ad esempio dati o risultati di calcoli analitici inseriti in un report;
- metadati: sono dati che descrivono gli attributi di altri dati specificandone il significato (struttura, elementi, relazioni) e il contesto, inclusa l'attribuzione a un individuo.

Ad es.: supponiamo di avere il dato *3.5*, esso da solo non è significativo, per qualificarlo occorrono i suoi metadati: *Cloruro di sodio, lotto 1234, 3.5 mg, P. Rossi 01/06/15*

Si noti che anche l'audit trail e l'eventuale firma elettronica sono metadati;

- copie conformi (*true copy*): sono copie esatte di un dato o record originale, quindi possono "sostituirlo". Inoltre possono essere mantenute anche in un formato diverso da quello in cui era stato generato il record originale (ad es. la scansione elettronica di un record cartaceo).
- riesame dei dati (*review, reporting and use*): i dati devono essere riesaminati. Dovrebbe dunque esistere una procedura che descrive tale riesame e l'approvazione dei dati, compresi i dati originali (*raw data*) e i relativi metadati, incluso l'audit trail.

Tale riesame deve essere documentato.

- conservazione (*retention and retrieval*): i dati devono essere disponibili durante tutto il periodo di conservazione richiesto dalle normative. Solitamente i dati vengono mantenuti "in linea", cioè sul sistema in uso corrente. Devono essere adottate le misure necessarie per proteggere i dati da perdite o alterazioni intenzionali o accidentali.

Se automatiche, queste misure devono essere state oggetto della convalida.

I dati in linea devono essere oggetto di backup per poter ripristinare il sistema in caso di eventi disastrosi;

- l'archiviazione si distingue dalla conservazione perché i dati vengono rimossi dal sistema in uso e spostati su un sistema che provvede alla loro indicizzazione e ne agevola la ricerca e il recupero, ma generalmente non consente la loro visualizzazione e quindi neppure la loro modifica e analisi o rielaborazione. In caso di necessità solitamente occorre ripristinarli sul sistema corrente per poterli consultare (*retrieval*).

Alla conclusione del periodo di conservazione, l'archiviazione termina con la cancellazione (*destruction*) del dato.

I requisiti della data integrity

Per essere considerati integri i dati devono soddisfare i seguenti requisiti (comunemente identificati con l'acronimo ALCOA), cioè devono essere:

- *attribuibili*: è possibile risalire a chi ha acquisito o inserito un dato o eseguito un'azione;
- *leggibili*: deve essere possibile leggere i dati e le registrazioni;
- *contemporanei*: documentati al momento della attività;
- *originali* (o "copie conformi"): un dato generato in elettronico o una copia con le stesse informazioni.

Dati in formato dinamico (formato elettronico elaborabile) vanno conservati in tale formato;

- *a disposizione* (*available*): per revisioni o verifiche ispettive per tutto il periodo di vita del record. Conservati su supporti elettronici duraturi e coperti da adeguate misure di protezione (backup, ridondanze ecc.).

Inoltre sono necessari i seguenti requisiti (ALCOA+ Plus) che sono comunque impliciti nei precedenti:

- *completi*: tutti i dati devono essere presenti e disponibili, ad esempio senza omissioni, cancellazioni o sovrascritture incluse ripetizioni di analisi;
- *consistenti*: i dati devono essere validi, ad esempio tutti gli elementi del record, come le sequenze di eventi, sono contrassegnati con data e ora nella sequenza attesa;
- *accurati*: privi di errori o con modifiche documentate (ad es. con audit trail);
- *disponibili*: per revisioni o verifiche ispettive per tutto il periodo di vita del record.

Principali misure della data integrity

Per soddisfare i requisiti sopra indicati le principali misure applicabili per i dati in formato elettronico sono le seguenti.

Credenziali di accesso al sistema univoche (logiche o biometriche). Oltre ad altre misure di sicurezza logica eventualmente applicabili, come:

- profili utente;
- privilegi sulle cartelle di rete e locali;
- antivirus;
- indipendenza degli amministratori;
- audit trail.

La revisione dei dati deve essere documentata e descritta in procedura, incluse azioni in caso di errori e omissioni. Essa deve considerare:

- risultati prossimi ai limiti di accettazione;
- modifiche ai metodi e ai parametri di processo prima dell'esecuzione;
- riprocessamento dei dati;
- modifiche manuali;
- audit trail (come parte integrante del processo di revisione delle registrazioni);
- esclusione di risultati dalle elaborazioni;
- correttezza e inalterabilità della data e ora (se usata in report o audit trail):
  - la data e ora dei sistemi devono essere corrette (rispetto a un riferimento ufficiale);
  - gli utenti finali non devono avere i privilegi per modificare la data-ora dei sistemi.

Deve esserci una copia di backup del software, ma soprattutto dei dati GxP critici, inclusi metadati e dati originali (raw data). Le modalità possono variare secondo la infrastruttura IT e il sistema, ma deve essere verificata la possibilità di ripristinare i dati (anche periodicamente).

Il soddisfacimento di queste misure deve essere verificato e documentato durante le attività di convalida iniziale del sistema e, ove necessario, riverificato periodicamente, ad esempio durante la verifica periodica dei sistemi (prevista dall'Annex 11) o gli audit interni del QA.

Conclusioni

Abbiamo visto che le linee guida GAMP 5 propongono i concetti base del ciclo di vita del software, delle categorie del software e dell'analisi dei rischi per pianificare ed eseguire le attività di convalida dei sistemi che svolgono funzioni a impatto diretto/indiretto sulla qualità del prodotto, dei quali occorre assicurare il "buon funzionamento", come richiesto dalle GMP.

Abbiamo poi utilizzato la linea guida GAMP sulla data integrity per esaminare i concetti fondamentali della governance dei dati, che a partire dalle definizioni del ciclo di vita dei dati (dati grezzi, metadati ecc.) e dei requisiti della data

integrity (ALCOA), portano alle misure da implementare sui sistemi per assicurarne la integrità in particolare dei dati in formato elettronico: accessi controllati, backup e restore, inalterabilità di data e ora ecc.

Attualmente gli sforzi dei promotori dei gruppi di lavoro GAMP sono rivolti all'emissione di nuove linee guida per adeguare al meglio i requisiti della data integrity alle varie tipologie di sistemi.

Ci auguriamo che questi nuovi documenti agevolino ancor più l'introduzione dei sistemi di Industry 4.0 nell'industria farmaceutica italiana, consentendole di rimanere all'avanguardia in questo settore così importante.

Bibliografia

Food and Drug Administration. *Guidelines of general principle of process validation,* 1987.

GAMP 5. *A risk-based approach to compliant GxP computerized systems.* ISPE© 2008.

ICH Harmonized tripartite guideline. *Quality risk management Q9*, 2005.

ISO 14971 Application of risk management to medical devices, 2000.

ISPE©GAMP. *Records and data integrity guide*, 2017.