Ann. Ist. Super. Sanità, vol. 33, n. 1 (1997), pp. 157-172

SERIE OCSE

su

PRINCIPI DI BUONA PRATICA DI LABORATORIO
E CONTROLLO DI CONFORMITÀ

Numero 10

Documento di consenso alla BPL

APPLICAZIONE DEI PRINCIPI DI BPL AI SISTEMI INFORMATICI

Monografia ambiente n. 116

Direttorato dell'Ambiente

ORGANIZZAZIONE PER LA COOPERAZIONE E LO SVILUPPO ECONOMICI

Parigi 1995

© OCSE, 1995
© Per l'edizione italiana: Istituto Superiore di Sanità, 1997

Il testo completo è disponibile on-line nella sua versione originale (in inglese e francese).

INDICE

PREMESSA

Nell'ambito della terza riunione di consenso sulla buona pratica di laboratorio dell'OCSE tenutasi dal 5 all'8 ottobre 1992, ad Interlaken, Svizzera, un Gruppo di esperti si è riunito per discutere l'interpretazione dei principi di BPL quando questi vengano applicati ai sistemi informatici. Il Gruppo di lavoro è stato presieduto dal Dr. Theo Helder dell'Autorità di controllo olandese di conformità alla BPL, Paesi Bassi. Il verbalizzatore è stato il Sig. Bryan Doherty (Presidente del Comitato informatico dell'Associazione britannica per l'assicurazione di qualità nella ricerca). I partecipanti al Gruppo di lavoro provenivano dagli organismi nazionali di controllo della conformità alla BPL e dai Centri di saggio dei seguenti Paesi: Austria, Belgio, Danimarca, Finlandia, Francia, Germania, Giappone, Paesi Bassi, Gran Bretagna, Svizzera, USA. Tale Gruppo di lavoro non è stato in grado di raggiungere l'accordo su un documento di guida dettagliato entro i tempi disponibili. Tuttavia, esso ha sviluppato un documento denominato "Concetti relativi ai sistemi informatici nell'ambito della BPL", che riporta i principi generali e descrive i temi ad essi associati. Tale documento è stato fatto circolare per parere tra i Paesi Membri.

Sulla base dei commenti ricevuti, il Gruppo di esperti della buona pratica di laboratorio, in occasione della quinta riunione del marzo 1993 ha ritenuto necessario svolgere ulteriore lavoro ed ha chiesto che venisse convocata una seconda riunione del Gruppo. Sotto la presidenza del Dr. Helder e con la presenza del Sig. Doherty in qualità di verbalizzatore, il Gruppo si è riunito a Parigi dal 14 al 16 dicembre 1994. Hanno partecipato i rappresentanti dei governi e delle industrie di Canada, Danimarca, Francia, Germania, Giappone, Paesi Bassi, Gran Bretagna, Svezia ed USA.

La bozza del documento di consenso sviluppata dal Gruppo di esperti si basava sul documento emerso dalla riunione di Interlaken, nonché dei relativi commenti ricevuti dai Paesi Membri e da un Gruppo di lavoro congiunto tra governo ed industria della Gran Bretagna. Successivamente tale documento è stato rivisto, modificato ed approvato dal Gruppo di esperti e dalla riunione congiunta del Gruppo chimico e del Comitato di gestione del Programma speciale per il controllo delle sostanze chimiche. Il Comitato per le politiche ambientali ha raccomandato che il documento venisse diffuso pubblicamente dietro autorizzazione del Segretario generale.

Documento di consenso alla BPL

APPLICAZIONE DEI PRINCIPI DI BPL AI SISTEMI INFORMATICI

Nel corso degli ultimi anni vi è stato un aumento dell'impiego dei sistemi informatici nei Centri di saggio che svolgono per la sicurezza della salute pubblica e dell'ambiente. Tali sistemi informatici possono essere utilizzati per acquisire direttamente o indirettamente dati, elaborarli, registrarli e conservarli e sempre di più come parte integrante di attrezzature automatizzate. Laddove i sistemi informatici sono associati alla conduzione di studi a scopo regolatorio, è indispensabile che essi siano sviluppati, convalidati, gestiti e mantenuti nel rispetto dei principi di buona pratica di laboratorio (BPL) dell'OCSE.

Settore di applicazione

Tutti i sistemi informatici utilizzati per ottenere, misurare o valutare dati a scopo regolatorio dovranno essere sviluppati, convalidati, gestiti e mantenuti secondo modalità conformi ai principi di BPL.

Durante la programmazione, l'esecuzione e la preparazione del rapporto degli studi possono essere utilizzati diversi sistemi informatici per varie finalità. Queste possono includere l'acquisizione elettronica diretta o indiretta dei dati, il funzionamento/controllo delle attrezzature automatizzate e l'elaborazione, la registrazione e l'immagazzinamento dei dati. Per tali diverse attività, i sistemi informatici possono coprire esigenze che vanno da strumento di programmazione analitica a elaboratore di calcolo personale, a sistema di gestione delle informazioni di laboratorio (SGIL) con funzioni multiple. Qualunque sia il livello di coinvolgimento del sistema informatico, dovranno comunque essere applicati i principi di BPL.

Impostazione

I sistemi informatici associati alla conduzione degli studi per fini regolatori dovranno essere realizzati adeguatamente, essere dimensionati opportunamente ed essere idonei agli scopi previsti. Dovranno essere in vigore procedure adatte a controllare e mantenere tali sistemi e questi dovranno essere sviluppati, convalidati e gestiti conformemente ai principi di BPL.

E' estremamente importante dimostrare che un sistema informatico sia adatto agli scopi previsti. Tale operazione viene denominata convalida.

Il procedimento di convalida fornisce un grado notevole di garanzia che un sistema informatico soddisfi caratteristiche prestabilite. La convalida dovrà essere attuata mediante un programma formale di convalida eseguito prima dell'impiego operativo.

Applicazione dei principi di BPL ai sistemi informatici

Le considerazioni che seguono saranno utili nell'applicazione dei principi di BPL ai sistemi informatici citati sopra:

1. Responsabilità

a) La *Direzione* di un Centro di saggio è responsabile globalmente della conformità generale ai principi di BPL. Tale responsabilità include la designazione e l'organizzazione pratica di un numero adeguato di persone opportunamente qualificate ed esperte, nonché l'obbligo di assicurare che le strutture, le attrezzature e le procedure di trattamento dei dati siano di standard adeguato.

La Direzione ha il compito di assicurare che i sistemi informatici siano adatti per gli scopi previsti. Essa dovrà stabilire norme e procedure in quest'ambito al fine di garantire che i sistemi siano sviluppati, convalidati, gestiti e mantenuti conformemente ai principi di BPL. La Direzione dovrà inoltre garantire che tali norme e procedure siano comprese e rispettate ed assicurare che abbia luogo l'effettivo controllo di tali requisiti.

La Direzione dovrà designare le persone incaricate di seguire lo sviluppo, la convalida, il funzionamento e la manutenzione dei sistemi informatici. Questo personale dovrà essere adeguatamente qualificato e dotato dell'esperienza e della formazione necessarie per svolgere i propri compiti in accordo ai principi di BPL.

b) I *Direttori degli studi* sono responsabili nel quadro dei principi di BPL della conduzione generale dei rispettivi studi. Dal momento che molti studi faranno uso di sistemi informatici, è indispensabile che i Direttori degli studi siano pienamente consapevoli del coinvolgimento di ciascun sistema informatico utilizzato negli studi sotto la loro direzione.

Per quanto attiene ai dati registrati elettronicamente, le responsabilità del Direttore dello studio sono le stesse previste per i dati registrati su carta e pertanto negli studi in BPL si dovranno utilizzare soltanto sistemi convalidati.

c) *Personale.* Tutto il personale che utilizza i sistemi informatici ha la responsabilità di gestirli in accordo ai principi di BPL. Il personale addetto allo sviluppo, convalida, funzionamento e manutenzione dei sistemi informatici deve svolgere queste attività in accordo ai principi di BPL ed a standard tecnici riconosciuti.

d) Le responsabilità dell'unità *di assicurazione di qualità* (AQ) relativamente ai sistemi informatici devono essere specificate dalla Direzione e codificate in norme e procedure scritte. Il programma di assicurazione di qualità dovrà includere procedure e prassi per assicurare il raggiungimento degli standard prefissati in tutte le fasi dei processi di convalida, funzionamento e manutenzione dei sistemi informatici. Inoltre, esso dovrà includere procedure e modalità per l'introduzione di sistemi commerciali e per l'elaborazione e lo sviluppo in sede di sistemi informatici.

Il personale addetto all'assicurazione di qualità è tenuto a controllare la conformità alla BPL dei sistemi informatici e dovrà essere addestrato per ogni tecnica specialistica necessaria. Dovrà conoscere tali sistemi in misura sufficiente da consentire pareri obiettivi; in taluni casi può rendersi necessario designare supervisori specializzati.

Il personale dell'AQ dovrà avere accesso diretto, per verifica, alla sola lettura dei dati immagazzinati in un sistema informatico.

2. Addestramento

I principi di BPL prevedono che un Centro di saggio disponga di personale qualificato ed esperto e di programmi di addestramento documentati, compreso l'addestramento sul luogo di lavoro e, quando opportuno, la frequenza a corsi di addestramento esterni. Di tali corsi dovrà essere mantenuta la documentazione.

I provvedimenti descritti dovranno valere anche per tutto il personale addetto ai sistemi informatici.

3. Impianti ed apparecchiature

Si dovrà disporre di impianti ed apparecchiature adeguati agli studi eseguiti in conformità ai principi di BPL. Per quanto riguarda i sistemi informatici dovranno essere fatte diverse considerazioni specifiche:

a) *Impianti*

Si dovrà dare la dovuta considerazione all'ubicazione fisica dei sistemi informatici, delle componenti periferiche, delle apparecchiature di comunicazione e dei mezzi di immagazzinamento elettronico. Valori estremi di temperatura e umidità, polvere, interferenze elettromagnetiche e vicinanza a cavi ad alta tensione dovranno essere evitati, a meno che le apparecchiature non siano concepite specificatamente per operare in tali condizioni.

Inoltre, si dovrà tenere conto della fornitura elettrica per le attrezzature elettroniche e, quando opportuno, dei gruppi di continuità o di sicurezza per i sistemi informatici, il cui guasto improvviso potrebbe influenzare i risultati di uno studio.

Dovranno essere predisposte attrezzature adeguate per la conservazione protetta dei mezzi di deposito elettronico dei dati.

b) *Apparecchiature*

i) *Componenti fisici e programmi*

Si definisce sistema informatico un gruppo di componenti fisici (hardware) e relativi programmi (software) concepito e costruito per svolgere una funzione o un gruppo di funzioni specifiche.

Lo hardware è costituito dai componenti fisici del sistema informatico; esso comprende l'unità di calcolo stessa e le sue componenti periferiche.

Il software è l'insieme dei programmi per il controllo delle operazioni svolte dal sistema informatico.

Tutti i principi di BPL relativi alle attrezzature vengono quindi applicati sia ai componenti fisici che ai programmi.

ii) *Comunicazioni*

Le comunicazioni relative ai sistemi informatici rientrano generalmente in due categorie: tra gli elaboratori stessi o tra elaboratori e componenti periferiche.

Tutti i dispositivi di comunicazione sono potenziali fonti di errore e possono determinare la perdita o l'alterazione dei dati. Durante le fasi di sviluppo, convalida, funzionamento e manutenzione di qualsiasi sistema informatico dovranno essere eseguiti controlli adeguati circa la sicurezza e l'integrità di detti sistemi.

4. Manutenzione e ripristino operativo a seguito di emergenze

Ogni sistema informatico dovrà essere installato e mantenuto in modo atto ad assicurare la continuità del suo perfetto funzionamento.

a) *Manutenzione*

Si dovrà disporre di procedure documentate riguardo alla manutenzione preventiva normale e alla riparazione dei guasti. Tali procedure dovranno specificare nei dettagli i ruoli e le responsabilità del personale coinvolto. Laddove le attività di manutenzione abbiano richiesto l'apporto di variazioni ai componenti fisici e/o al programma, è consigliabile convalidare di nuovo il sistema. Durante il funzionamento quotidiano del sistema dovrà essere conservata documentazione di tutti i problemi o di incompatibilità individuati e delle misure correttive adottate.

b) *Ripristino operativo a seguito di emergenze*

Dovranno essere istituite procedure che descrivano le misure da adottare allorquando si verificano guasti parziali o totali di un sistema informatico. Tali misure possono variare dalla duplicazione pianificata di componenti fisici al ripristino dei sistemi cartacei. Tutti i piani di emergenza dovranno essere documentati e convalidati, dovranno assicurare l'integrità ininterrotta dei dati e non dovranno compromettere lo studio in alcun modo. Il personale partecipante alla conduzione degli studi in BPL dovrà essere a conoscenza di tali piani di emergenza.

Le procedure da adottare per il ripristino di un sistema informatico dipenderanno dalla criticità del sistema, ma è indispensabile conservare le copie di riserva di tutti i programmi. Se le procedure di ripristino richiedono variazioni alla macchina o al programma occorrerà convalidare di nuovo il sistema.

5. Dati

Secondo i principi di BPL i dati grezzi sono costituiti da tutte le registrazioni e le documentazioni originali di laboratorio, compresi i dati immessi direttamente in un elaboratore di calcolo per mezzo di un'interfaccia strumentale, quali i risultati di osservazioni originali e delle attività in uno studio e che servono per la ricostruzione e la valutazione del rapporto di quello studio.

I sistemi informatici che operano in conformità alla BPL possono essere associati ai dati grezzi in molte forme, ad esempio su mezzi elettronici di deposito, calcolatori o stampanti collegate ad apparecchiature e copie su microfilm e microfiche. Occorre che venga definito cosa si intende per dati grezzi per ogni sistema informatico.

Quando i sistemi informatici vengono utilizzati per acquisire, elaborare, registrare o immagazzinare dati elettronicamente, la struttura del sistema dovrà sempre garantire la conservazione dell'intero percorso di verifica per mostrare tutte le variazioni apportate ai

dati senza celare i dati originali. Dovrà essere possibile associare tutte le variazioni apportate alle persone che hanno proceduto al cambiamento per mezzo di firme (elettroniche) congiuntamente a ora e data. Dovrà essere indicato il motivo della modifica.

Se i dati grezzi sono conservati elettronicamente occorre predisporre le condizioni per la conservazione a lungo termine per il tipo di dati disponibili e per la durata prevista del sistema informatico. Le variazioni nei componenti fisici o di programma debbono essere fatte in modo da garantire l'accesso permanente ai dati grezzi e la loro conservazione senza comprometterne l'integrità.

Le informazioni di supporto come i manuali di manutenzione e le registrazioni delle calibrazioni, necessarie per verificare la validità dei dati grezzi o per permettere la ricostruzione di un procedimento o di uno studio, dovranno essere conservate negli archivi.

Le procedure relative al funzionamento di un sistema informatico dovranno anche descrivere procedure alternative per acquisire dati in caso di guasti del sistema. In simili circostanze qualsiasi dato grezzo registrato manualmente ed immesso in seguito nel calcolatore dovrà essere identificato chiaramente come tale e dovrà essere conservato come documentazione originale. Le procedure manuali di duplicazione dovranno servire per ridurre al minimo il rischio di perdita dei dati ed assicurare che tali documentazioni alternative siano conservate.

Se l'invecchiamento del sistema determina l'esigenza di trasferire i dati elettronici da un sistema ad un altro, tale processo deve essere ben documentato e si dovrà verificarne l'integrità. Laddove non sia possibile procedere al trasferimento, i dati grezzi dovranno essere riportati in un altro mezzo per produrne una copia esatta che va verificata prima di procedere alla distruzione delle documentazioni elettroniche originali.

6. Sicurezza

Dovranno essere istituite procedure per proteggere i componenti fisici, il programma e i dati da alterazioni o variazioni non autorizzate, o da perdite. In quest'ottica le misure di sicurezza prevedono che venga impedito l'accesso o le variazioni non autorizzati al sistema informatico e ai dati conservati in quel sistema. Dovrà essere valutato il rischio di alterazione dei dati dovuta a virus o ad altre cause e dovranno essere adottate misure di sicurezza anche per garantire l'integrità dei dati nei casi di guasti sia a lungo che a breve termine.

a) *Sicurezza fisica*

Dovranno essere in vigore misure di sicurezza fisica per consentire l'accesso al calcolatore, ai dispositivi di comunicazione, alle componenti periferiche e ai mezzi di immagazzinamento elettronico soltanto al personale autorizzato. Per le apparecchiature che non sono collocate all'interno di "locali specifici per calcolatori" (ad esempio, i calcolatori personali e i terminali), bisogna almeno istituire dei controlli standard per l'accesso al Centro di saggio. Tuttavia, se tali apparecchiature sono collocate a distanza (ad esempio, i componenti portatili e i collegamenti modem), dovranno essere adottate misure aggiuntive.

b) *Sicurezza logica*

Per ogni sistema informatico o sua applicazione debbono essere in vigore misure di sicurezza logica al fine di impedire l'accesso non autorizzato al sistema informatico, alle applicazioni e ai dati. E' indispensabile garantire che vengano utilizzate soltanto versioni

di programmi approvate e convalidate. La sicurezza logica può implicare l'esigenza di adottare un'unica identità di utente con una parola di accesso associata. Qualsiasi introduzione di dati o di programmi da fonti esterne dovrà essere controllata. Tali controlli possono essere forniti dal sistema operativo dell'elaboratore mediante procedure di sicurezza specifiche, procedure incluse nelle applicazioni o combinazioni di entrambe.

c) *Integrità dei dati*

Essendo il mantenimanto dell'integrità dei dati un obiettivo primario dei principi di BPL, è importante che chiunque venga a contatto con i sistemi informatici sia consapevole della necessità di rispettare le condizioni di sicurezza suddette. La Direzione dovrà garantire che il personale sia consapevole dell'importanza della sicurezza dei dati, delle procedure e delle caratteristiche dei sistemi disponibili per fornire il grado di sicurezza necessario. Le caratteristiche dei sistemi potrebbero implicare la sorveglianza dei sistemi di accesso, l'adozione di procedure per il controllo dei documenti e la redazione di rapporti relativi alle eccezioni e/o agli andamenti.

d) *Duplicazione*

Normalmente vengono create delle copie di riserva di tutti i programmi e dei dati al fine di permettere il ripristino dei sistemi a seguito di guasti che possono compromettere l'integrità del sistema, come il danneggiamento del disco. Ciò implica, quindi, che le copie di riserva possono divenire a loro volta dati grezzi e che devono essere trattati come tali.

7. Convalida dei sistemi informatici

I sistemi informatici debbono essere adatti agli scopi previsti. Si dovrà tenere conto dei seguenti aspetti:

a) *Accettazione*

I sistemi informatici dovranno essere concepiti per soddisfare i principi di BPL ed attuati secondo uno schema predefinito. Si dovrà disporre della documentazione indicante che i sistemi sono stati sviluppati in modo controllato e preferibilmente secondo standard tecnici e di qualità riconosciuti (ad esempio ISO/9001). Inoltre, dovranno essere fornite le prove che il sistema è stato esaminato dal Centro di saggio per valutarne la conformità con i criteri di accettazione, prima di essere messo in funzione. Le prove di accettazione formale richiedono la conduzione di esami secondo un programma predefinito e la conservazione delle prove documentate di tutte le procedure di saggio, dei dati dei saggi, dei risultati dei saggi, di un riassunto formale dei saggi eseguiti e di documentazione dell'accettazione formale.

Per quanto attiene ai sistemi acquistati da un rivenditore è probabile che la documentazione raccolta durante le fasi di sviluppo sia conservata da quest'ultimo. In questo caso il Centro di saggio dovrà disporre di documentazione a supporto della valutazione formale e/o delle verifiche eseguite dal rivenditore.

b) *Valutazione retrospettiva*

Vi potranno essere sistemi per i quali non è stata prevista o menzionata la conformità ai principi di BPL. Qualora si verifichi questo, per l'impiego di tali sistemi dovrà essere fornita una giustificazione documentata; ciò dovrà includere una valutazione retrospettiva per valutarne l'idoneità.

La valutazione retrospettiva ha inizio con la raccolta di tutta la documentazione cronologica relativa ai sistemi informatici. Detta documentazione viene poi riesaminata e riassunta per iscritto. Il riassunto della valutazione retrospettiva dovrà specificare quali prove di convalida esistono e quali dovranno essere effettuate in futuro per assicurare la convalida del sistema informatico.

c) *Controllo delle variazioni*

Il controllo delle variazioni è costituito dall'approvazione e dalla documentazione formali di tutti i cambiamenti apportati ai sistemi informatici durante la vita operativa del sistema. Tale controllo è necessario quando un cambiamento è potenzialmente in grado di influenzare lo stato di convalida di un sistema informatico. Le procedure per il controllo delle variazioni devono essere disponibili dal momento che il sistema informatico viene reso operativo.

Le procedure dovranno descrivere il metodo di valutazione atto a determinare la necessità di ripetere le prove necessarie a mantenere lo stato di convalida del sistema. Le procedure per il controllo delle variazioni dovranno identificare i responsabili delle stesse ai fini della determinazione della necessità del controllo delle modifiche e della loro approvazione.

d) *Meccanismi di supporto*

Allo scopo di assicurare che un sistema informatico continui ad essere idoneo per gli obiettivi previsti dovranno essere in vigore meccanismi di supporto per garantire che il sistema funzioni e sia utilizzato in modo corretto. Ciò può comportare la gestione, l'addestramento, la manutenzione, il supporto tecnico, la verifica e/o la valutazione delle prestazioni del sistema. La valutazione delle prestazioni è l'esame formale di un sistema ad intervalli periodici al fine di assicurare che esso continui a soddisfare i criteri di prestazione prestabiliti, come l'affidabilità, la sensibilità ed il dimensionamento.

8. Documentazione

Le voci sottoelencate forniscono una guida alla documentazione minima richiesta per lo sviluppo, la convalida, il funzionamento e la manutenzione dei sistemi informatici.

a) *Norme*

Dovranno esistere norme scritte di gestione concernenti, *inter alia*, l'acquisizione, i requisiti, lo schema, la convalida, le prove, l'installazione, il funzionamento, la manutenzione, il personale addetto, il controllo, la verifica, la sorveglianza e la rimozione dei sistemi informatici.

b) *Descrizione delle applicazioni*

Per ciascuna applicazione si dovrà disporre della documentazione che indichi esaurientemente:

- il nome del programma di applicazione o il codice d'identificazione e una descrizione chiara e dettagliata degli scopi dell'applicazione;
- i componenti fisici (con i numeri del modello) su cui operano i programmi di applicazione;
- il sistema operativo e gli altri programmi di sistema (ad esempio strumenti) utilizzati insieme alle applicazioni;

- il(i) linguaggio(i) di programmazione applicato(i) e/o gli strumenti delle basi di dati utilizzati;
- le funzioni principali eseguite dall'applicazione;
- una rassegna del tipo e dell'insieme di dati /schemi di basi di dati associati alle applicazioni;
- struttura dei documenti, messaggi di errore e di allarme e algoritmi associati alle applicazioni;
- i componenti del programma di applicazione con il numero della versione;
- la configurazione ed i dispositivi di comunicazione tra i moduli dell'applicazione e verso la strumentazione e gli altri sistemi.

c) *Codice di origine*

Alcuni Paesi Membri dell'OCSE prevedono che il codice di origine per i programmi di applicazione sia disponibile presso il, o possa essere rintracciabile dal, Centro di saggio.

d) *Procedure Operative Standard (POS)*

Buona parte della documentazione relativa all'utilizzazione dei sistemi informatici sarà redatta nella forma di POS. Queste dovranno coprire, ma non essere limitate a, gli aspetti che seguono:

- procedure relative al funzionamento dei sistemi informatici (componenti fisici/ programma), e le responsabilità del personale addetto;
- procedure per le misure di sicurezza utilizzate per individuare ed impedire l'accesso e le variazioni non autorizzati ai programmi;
- procedure ed autorizzazione per le modifiche ai programmi e documentazione di tali variazioni;
- procedure per le prove periodiche sul corretto funzionamento dell'intero sistema o dei suoi componenti e la documentazione di tali prove;
- procedure per la manutenzione dei sistemi informatici e di tutte le apparecchiature associate ad essi;
- procedure per lo sviluppo dei programmi e per le prove di accettazione, nonché per la documentazione di tutte le prove di accettazione;
- procedure di duplicazione per tutti i dati immagazzinati e per i piani di emergenza in caso di guasto;
- procedure per l'archiviazione e la rintracciabilità di tutti i documenti, i programmi e i dati del calcolatore;
- procedure per il controllo e la verifica dei sistemi informatici.

9. Archivi

I principi di BPL relativi all'archiviazione dei dati debbono essere applicati in modo coerente a tutti i tipi di dati. E' quindi importante che i dati elaborati elettronicamente siano immagazzinati con gli stessi livelli di controllo dell'accesso, di indicizzazione e di efficiente consultazione come per gli altri tipi di dati.

Laddove i dati elettronici di più studi siano immagazzinati su un singolo supporto di deposito (ad esempio, disco o nastro), ne sarà richiesto un elenco dettagliato.

Potrà essere necessario fornire dispositivi con controlli ambientali specifici atti ad assicurare l'integrità dei dati immagazzinati elettronicamente. Qualora ciò richiedesse dispositivi per l'archiviazione la Direzione dovrà garantire che il personale responsabile della gestione degli archivi sia identificato e che l'accesso ai locali sia limitato al personale autorizzato. Inoltre, sarà necessario attuare procedure per assicurare che non venga compromessa l'integrità a lungo termine dei dati immagazzinati. Qualora si prevedano problemi per l'accesso a lungo termine ai dati o quando i sistemi informatici debbono essere rimossi, dovranno essere stabilite procedure per assicurare che sia garantita la leggibilità permanente dei dati. Ciò può implicare, ad esempio, la realizzazione di copie cartacee o il trasferimento dei dati ad un altro sistema.

Nessun dato immagazzinato elettronicamente dovrà essere distrutto senza l'autorizzazione della Direzione e la documentazione relativa. Altri dati conservati come supporto ai sistemi informatici, quali il codice di origine e la documentazione relativa a sviluppo, convalida, funzionamento, manutenzione e controllo, dovranno essere conservati almeno per la durata prevista per la documentazione degli studi associati a tali sistemi.

Definizione dei termini [1]

Codice d'origine. - Un programma informatico originale espresso in forma leggibile per l'operatore (linguaggio di programmazione) che deve essere tradotto in forma leggibile per il sistema prima che questo possa essere eseguito dal calcolatore.

Componenti periferici. - Ogni strumentazione interfacciata o i componenti ausiliari o remoti, come le stampanti, i modem, i terminali, ecc.

Controllo delle variazioni. - Valutazione e documentazione correnti delle operazioni del sistema e delle modifiche al fine di determinare se occorra un procedimento di convalida in seguito a variazioni apportate al sistema informatico.

Convalida di un sistema informatico. - La dimostrazione dell'idoneità di un sistema informatico per gli scopi previsti.

Criteri di accettazione. - Criteri codificati che dovranno essere rispettati per completare efficacemente una fase di un saggio o per soddisfare i requisiti di consegna.

Firma elettronica. - L'inserimento sotto forma di impulsi magnetici o di compilazione di dati al calcolatore di ogni simbolo, o serie di simboli, eseguito, adattato o autorizzato da una persona come equivalente alla firma manuale della stessa.

Hardware. - Le componenti fisiche di un sistema informatico, incluso lo stesso calcolatore e i suoi componenti periferici.

---

[1] Ulteriori definizioni dei termini sono contenute nei "Principi di buona pratica di laboratorio dell'OCSE", numero 1 di questa serie OCSE sui principi di BPL e controllo di conformità (pag. 1-25).

Prove di accettazione. - Prove formali su un sistema informatico nell'ambiente operativo previsto al fine di determinare se tutti i criteri di accettazione del Centro di saggio siano rispettati e se il sistema sia adatto a svolgere le operazioni richieste.

Sicurezza. - La protezione dei componenti fisici del calcolatore e dei suoi programmi dall'accesso, l'utilizzazione, la modifica, la distruzione o l'apertura accidentali o intenzionali. La sicurezza riguarda anche il personale, i dati, le comunicazioni e la protezione fisica e logica delle installazioni del calcolatore.

Sistema informatico. - Un gruppo di componenti fisici o del programma associato, concepito e montato per eseguire una funzione specifica o un gruppo di funzioni.

Sistemi di duplicazione. - Misure idonee al ripristino dei documenti o dei programmi, per la ripresa dell'elaborazione o per l'utilizzazione di calcolatori alternativi a seguito di un guasto al sistema o di suo completo collasso.

Software (applicazioni). - Un programma acquisito o sviluppato, adattato a o predisposto per le necessità del Centro di saggio allo scopo di controllare i procedimenti, la raccolta dei dati, la manipolazione dei dati e la documentazione e/o archiviazione dei dati.

Software (sistema operativo). - Un programma o una serie di programmi, procedure e sottoprocedure utili a controllare le operazioni del calcolatore. Un sistema operativo può fornire servizi quali l'allocazione delle risorse, la programmazione, il controllo delle informazioni in ingresso/uscita e la gestione dei dati.

Standard tecnici riconosciuti. - Gli standard stabiliti dagli organismi nazionali o internazionali responsabili (ISO, IEEE, ANSI, ecc.).