ANEXA 11
SISTEME COMPUTERIZATE

Principiu

Această anexă se aplică tuturor formelor de sisteme computerizate utilizate ca parte a activităţilor reglementate de BPF. Un sistem computerizat este un set de componente de hardware şi software, care împreuna îndeplinesc anumite funcţionalităţi. Aplicaţia trebuie validată; infrastructura IT trebuie calificată. Când un sistem computerizat înlocuieşte o operaţie manuală nu trebuie să rezulte o scădere a calităţii produsului, a controlului procesului sau a asigurării calităţii. Nu trebuie să existe nicio creştere a riscului general pe care îl prezintă procesul.

Generalităţi

1. Managementul riscului

Managementul riscului trebuie aplicat pe toată durata de viaţă a sistemului computerizat, ţinând cont de siguranţa pacientului, integritatea datelor şi calitatea produsului. Ca parte a sistemului de management al riscului, deciziile în ceea ce priveşte extinderea validării şi controlul integrităţii datelor trebuie să se bazeze pe o evaluare de risc justificată şi documentată a sistemului computerizat.

2. Personal

Trebuie să existe cea mai strânsă cooperare între personalul relevant (cum ar fi proprietarul de proces, proprietarul de sistem, persoanele calificate) şi personalul IT.

3. Furnizori şi furnizori de servicii

3.1 Atunci când, pentru a furniza, instala, configura, valida, întreţine (de ex. prin acces de la distanţă), modifica sau menţine un sistem computerizat sau serviciu înrudit sau pentru a procesa datele se utilizează terţe părţi (de ex. furnizori, furnizori de servicii), trebuie să existe acorduri oficiale între fabricant şi orice terţă parte, iar aceste acorduri trebuie să includă prevederi clare referitoare la responsabilităţile terţei părţi. Departamentele IT trebuie considerate a fi similare.
3.2 Competenţa şi siguranţa unui furnizor sunt factori cheie atunci când se alege un produs sau furnizor de serviciu. Necesitatea efectuării unui audit trebuie să se bazeze pe o evaluare de risc.
3.3 Documentaţia furnizată cu produsele comerciale trebuie revizuită de către utilizatori pentru a se verifica dacă cerinţele acestora sunt îndeplinite.
3.4 Sistemul calităţii şi informaţiile obţinute din audit referitoare la furnizori sau dezvoltatori de software şi sisteme implementate trebuie să fie disponibile pentru inspectori, dacă sunt solicitate.

Faza de proiectare

4. Validare

4.1 Documentaţia şi rapoartele de validare trebuie să acopere etapele relevante ale ciclului de viaţă. Fabricanţii trebuie să poată justifica standardele, protocoalele, criteriile de acceptare, procedurile şi înregistrările lor, pe baza evaluării riscului.

4.2 Documentaţia de validare trebuie să includă înregistrări de control al schimbărilor (dacă este cazul) şi rapoarte ale oricăror deviaţii observate în timpul procesului de validare.

4.3 Trebuie să fie disponibilă o listă actualizată a tuturor sistemelor relevante şi funcţionalitatea lor din punct de vedere al BPF (inventar).
Pentru sistemele critice trebuie să fie disponibilă o descriere la zi a sistemului care să detalieze amplasarea fizică şi logică, fluxurile de date şi interfeţele cu alte sisteme sau procese, orice hardware şi software necesar şi măsurile de securitate.

4.4 Specificarea cerinţelor utilizatorilor trebuie să descrie funcţiile solicitate ale sistemului computerizat şi să se bazeze pe o evaluare de risc documentată şi pe impactul asupra BPF. Cerinţele utilizatorilor trebuie să poată fi urmărite pe toată durata de viaţă.

4.5 Utilizatorii trebuie să ia toate măsurile rezonabile pentru a se asigura că sistemul a fost dezvoltat în acord cu un sistem adecvat de management al calităţii.

4.6 Pentru validarea sistemelor computerizate făcute la comandă sau personalizate trebuie să existe un proces care să asigure evaluarea formală şi raportarea calităţii şi a performanţelor pentru întreaga perioadă de viaţă a sistemului.

4.7 Trebuie să se demonstreze că există metode de testare adecvate şi scenarii de testare. În mod special, trebuie luate în considerare limitele parametrilor sistemului (procesului), limitele datelor şi modul de tratare al erorilor. Pentru instrumentele de testare automate şi mediile de testare trebuie să existe evaluări documentate privind adecvarea lor.

4.8 Dacă datele sunt transferate într-un alt format de date sau în alt sistem, validarea trebuie să includă verificări că datele nu au fost alterate în timpul procesului de migrare, în ceea ce priveşte valoarea şi/sau sensul lor.

Faza Operaţională

5. Date

Sistemele computerizate care schimbă date electronice cu alte sisteme trebuie să includă verificări interne în ceea ce priveşte introducerea şi procesarea corectă a datelor, cu scopul micşorării riscului.

6. Verificări ale acurateţii

Pentru datele critice introduse manual, trebuie să existe o verificare suplimentară a acurateţii datelor. Această verificare poate fi efectuată de către un al doilea operator sau prin mijloace electronice validate. Potenţialele consecinţe ale introducerii de date eronate sau incorecte în sistem şi criticalitatea acestora trebuie să fie evaluate prin managementul riscului.

7. Stocarea de date

7.1 Datele trebuie să fie securizate împotriva deteriorării, atât prin mijloace fizice, cât şi electronice. Datele stocate trebuie să fie verificate în ceea ce priveşte accesibilitatea, lizibilitatea şi acurateţea. Accesul la date trebuie să fie asigurat pe toată perioada lor de păstrare.

7.2 Trebuie să se efectueze salvări regulate ale datelor relevante. Integritatea şi acurateţea datelor salvate şi posibilitatea de a restabili datele trebuie verificată în timpul validării şi monitorizată periodic.

8. Documente imprimate

8.1 Trebuie să fie posibil să se obţină copii imprimate, clare, ale datelor stocate electronic.

8.2 Pentru înregistrări care fac parte din eliberarea seriei trebuie să fie posibilă generarea de documente imprimate care să indice dacă datele au fost modificate de la introducerea originală.

9. Audit Trails

Pe baza evaluării riscului, trebuie să se ia în considerare includerea în sistem a unei înregistrări privind toate schimbările şi ştergerile datelor relevante din punct de vedere al BPF (un „audit trail” generat de sistem). În cazul schimbărilor şi ştergerilor datelor relevante din punct de vedere al BPF, motivul trebuie documentat. „Audit trails” trebuie să fie disponibile şi convertibile într-o formă general inteligibilă şi trebuie revizuite regulat.

10. Managementul schimbărilor şi al configuraţiilor

Orice schimbări ale unui sistem computerizat, inclusiv ale configurărilor sistemului trebuie făcute într-o manieră controlată, în acord cu o procedură definită.

Evaluare periodică
Sistemele computerizate trebuie evaluate periodic pentru a confirma că îşi menţin starea validată şi sunt conforme cu BPF. Astfel de evaluări trebuie să includă, unde este cazul, gama curentă de funcţionalităţi, înregistrări ale deviaţiilor, incidente, probleme, istoricul actualizărilor, performanţa, acurateţea, securitatea şi rapoarte referitoare la statutul validării.

12. Securitate

12.1 Trebuie să existe controale fizice şi/sau logice pentru a restricţiona accesul la sistemul computerizat numai pentru persoanele autorizate. Metode adecvate de a preveni accesul neautorizat la sistem pot include utilizarea de chei, carduri de acces, coduri personale cu parole, date biometrice, restricţionarea accesului la echipamentul computerului şi la zona de stocare a datelor.
12.2 Extinderea controalelor de securitate depinde de cât de critic este sistemul computerizat.
12.3 Crearea, schimbarea şi anularea autorizaţiilor de acces trebuie înregistrate.
12.4 Sistemele de management al datelor şi documentelor trebuie proiectate pentru a înregistra identitatea operatorilor care introduc, schimbă, confirmă sau şterg date, inclusiv data şi timpul.

13. Managementul incidentelor

Toate incidentele, nu doar eşecul sistemelor şi eroarea datelor, trebuie raportate şi evaluate.
Cauza care a provocat un incident critic trebuie identificată şi trebuie să stea la baza acţiunilor corective şi preventive.

14. Semnătura electronică

Înregistrările electronice pot fi semnate electronic. Este de aşteptat ca semnăturile electronice:

a. să aiba acelaşi impact ca semnăturile olografe în cadrul companiei;

b. să fie legate în mod permanent de înregistrările respective;

c. să includă ora şi data când s-au aplicat.

15. Eliberarea seriei

Atunci când un sistem computerizat este utilizat pentru a înregistra certificarea şi eliberarea seriei, sistemul trebuie să permită numai persoanei calificate să certifice eliberarea seriei şi trebuie să identifice şi să înregistreze persoana care eliberează sau certifică seriile. Acest lucru trebuie făcut prin utilizarea unei semnături electronice.

16. Continuitatea activităţii

Pentru disponibilitatea sistemelor computerizate care susţin procese critice, trebuie luate măsuri care să asigure continuitatea acelor procese în cazul unui eşec al sistemului (de ex. sisteme manuale sau alternative). Timpul necesar pentru a pune în funcţiune aceste mijloace alternative trebuie să se bazeze pe risc şi să fie adecvat pentru un anumit sistem şi pentru procesul pe care îl susţine. Aceste aranjamente trebuie să fie adecvat documentate şi testate.

17. Arhivarea

Datele pot fi arhivate. Aceste date trebuie verificate în ceea ce priveşte accesibilitatea, lizibilitatea şi integritatea. Dacă trebuie făcute schimbări relevante sistemului (de ex. echipamentul computerului sau programele), atunci trebuie să se asigure şi să se testeze posibilitatea recuperării datelor.

Glosar

Aplicaţie: Software instalat pe o platformă/hardware definită, care asigură o funcţionalitate specifică.

Sisteme computerizate făcute la comandă/personalizate: Un sistem computerizat proiectat individual pentru a se potrivi unui proces specific.

Software comercial: Software disponibil comercial, a cărui adecvare pentru utilizare a fost demonstrată de un spectru larg de utilizatori.

Infrastructură IT: Hardware şi software cum ar fi software pentru reţea şi sisteme de operare, care fac posibilă funcţionarea aplicaţiei.

Ciclu de viaţă: Toate etapele din viaţa sistemului, de la cerinţele iniţiale până la retragerea sa, incluzând proiectarea, specificaţia, programarea, testarea, instalarea, operarea şi întreţinerea.

Proprietar de proces: Persoana responsabilă pentru proces.

Proprietar de sistem: Persoana responsabilă de disponibilitatea şi întreţinerea unui sistem computerizat şi de securitatea datelor din sistem.

Părţi terţe: Părţi care nu sunt în mod direct gestionate de către deţinătorul autorizaţiei de fabricaţie şi/sau import.