EURÓPAI BIZOTTSÁG
EGÉSZSÉG- ÉS FOGYASZTÓÜGYI FŐIGAZGATÓSÁG

Népegészségügy és kockázatértékelés
Gyógyszerek

Brüsszel,
SANCO/C8/AM/sl/ares(2010) 1064599

EudraLex
A gyógyszerekre vonatkozó szabályok az Európai Unióban

Kötet
Helyes gyártási gyakorlat
Emberi és állatgyógyászati felhasználásra szánt termékek

11. melléklet: Számítógépes rendszerek

A részletes iránymutatások közzétételének jogalapja: Az emberi felhasználásra szánt gyógyszerek közösségi kódexéről szóló 2001/83/EK irányelv 47. cikke és az állatgyógyászati készítmények közösségi kódexéről szóló 2001/82/EK irányelv 51. cikke. Ez a dokumentum iránymutatást nyújt az emberi felhasználásra szánt gyógyszerekről szóló 2003/94/EK irányelvben és az állatgyógyászati felhasználásra szánt gyógyszerekről szóló 91/412/EGK irányelvben meghatározott helyes gyártási gyakorlat (GMP) elveinek és iránymutatásainak értelmezéséhez.

A dokumentum státusza:változat

Javítás oka:a melléklet felülvizsgálatára a számítógépes rendszerek fokozott használata és e rendszerek megnövekedett összetettsége miatt került sor. A GMP-útmutató 4. fejezetéhez kapcsolódó módosításokat is javasolunk.

Az érvénybelépés határideje:2011. június 30.

Európai Bizottság, B-1049 Bruxelles/Europese Commissie, B-1049 Brussel
— BelgiumTelefon:
(32-2) 299 11 11

Alapelv

Ez a melléklet a szabályozott GMP-tevékenységek részeként használt számítógépes rendszerek valamennyi formájára vonatkozik. A számítógépes rendszer szoftver- és hardverelemek együttese, amelyek együttesen látnak el bizonyos funkciókat.

Az alkalmazásokat validálni kell; Az informatikai infrastruktúrának kvalifikáltnak kell lennie.

Amennyiben egy számítógépes rendszer egy manuális művelet helyébe lép, a termékminőség, a folyamatellenőrzés vagy a minőségbiztosítás nem csökkenhet. A folyamat általános kockázata nem növekedhet.

Általános

1. ***Kockázatértékelés***

A kockázatkezelést a számítógépes rendszer teljes életciklusa során alkalmazni kell, figyelembe véve a betegbiztonságot, az adatintegritást és a termékminőséget. A kockázatkezelési rendszer részeként a validálási és adatintegritási ellenőrzések mértékére vonatkozó döntéseknek a számítógépes rendszer indokolt és dokumentált kockázatértékelésén kell alapulniuk.

2. ***Személyzet***

Szoros együttműködésre van szükség az érintett személyzet – például a folyamattulajdonos, a rendszertulajdonos, a minősített személyek és az informatika – között. A személyzet minden tagjának rendelkeznie kell a rábízott feladatok ellátásához szükséges megfelelő képesítéssel, hozzáférési szinttel és meghatározott felelősségi körökkel.

3. ***Szállítók és szolgáltatók***

3.1 Amennyiben harmadik feleket (pl. szállítókat, szolgáltatókat) használnak fel pl. szolgáltatásnyújtásra, telepítésre, konfigurálásra, integrálásra, érvényesítésre, karbantartásra (pl. távoli hozzáférés révén), számítógépes rendszer vagy kapcsolódó szolgáltatás módosítására vagy fenntartására, illetve adatfeldolgozásra, hivatalos megállapodásoknak kell létezniük a gyártó és bármely harmadik fél között, és e megállapodásoknak egyértelműen tartalmazniuk kell a harmadik fél felelősségi körére vonatkozó nyilatkozatokat. Az informatikai osztályokat analógnak kell tekinteni.

3.2 A szállító szakértelme és megbízhatósága kulcsfontosságú tényező a termék vagy szolgáltató kiválasztásakor. Az ellenőrzés szükségességét kockázatértékelés alapján kell megállapítani.

3.3 A kereskedelemben kapható, kész termékeket tartalmazó dokumentációt a szabályozott felhasználóknak felül kell vizsgálniuk annak ellenőrzése érdekében, hogy teljesülnek-e a felhasználói követelmények.

3.4 A szoftver és a megvalósított rendszerek szállítóira vagy fejlesztőire vonatkozó minőségbiztosítási és ellenőrzési információkat kérésre az ellenőrök rendelkezésére kell bocsátani.

Projektszakasz

4. ***Validálás***

4.1 Az érvényesítési dokumentációnak és jelentéseknek ki kell terjedniük az életciklus releváns lépéseire. A gyártóknak képesnek kell lenniük arra, hogy kockázatértékelésük alapján megindokolják szabványaikat, protokolljaikat, elfogadási kritériumaikat, eljárásaikat és nyilvántartásaikat.
4.2 A validálási dokumentációnak (adott esetben) tartalmaznia kell a változás-ellenőrzési feljegyzéseket és a validálási folyamat során észlelt eltérésekről szóló jelentéseket.

4.3 A releváns rendszerek és azok GMP-funkciói (leltár) naprakész jegyzékének rendelkezésre kell állnia.

A kritikus rendszerek esetében rendelkezésre kell állnia egy naprakész rendszerleírásnak, amely részletezi a fizikai és logikai megoldásokat, az adatáramlást és a más rendszerekkel vagy folyamatokkal való interfészeket, a hardverre és a szoftverre vonatkozó előfeltételeket, valamint a biztonsági intézkedéseket.

4.4 A felhasználói követelményekre vonatkozó előírásoknak le kell írniuk a számítógépes rendszer szükséges funkcióit, és dokumentált kockázatértékelésen és a helyes gyártási gyakorlat (GMP) hatásán kell alapulniuk. A felhasználói igényeknek a teljes életciklus során nyomon követhetőknek kell lenniük.

4.5 A szabályozott felhasználónak minden ésszerű lépést meg kell tennie annak biztosítása érdekében, hogy a rendszert a megfelelő minőségirányítási rendszerrel összhangban fejlesztették ki. A szállítót megfelelően értékelni kell.

4.6 Az egyedi vagy személyre szabott számítógépes rendszerek validálásához olyan folyamatra van szükség, amely biztosítja a minőségre és a teljesítményre vonatkozó intézkedéseknek a rendszer valamennyi életciklus-szakaszára kiterjedő hivatalos értékelését és jelentését.

4.7 Bizonyítani kell a megfelelő vizsgálati módszerek és vizsgálati forgatókönyvek meglétét. Különösen a rendszer (folyamat) paraméterhatárait, az adathatárokat és a hibakezelést kell figyelembe venni. Az automatizált vizsgálati eszközöknek és vizsgálati környezeteknek dokumentált értékelésekkel kell rendelkezniük megfelelőségük tekintetében.

4.8 Ha az adatokat más adatformátumba vagy rendszerbe továbbítják, az érvényesítés során ellenőrizni kell, hogy az adatok értéke és/vagy jelentése nem változott-e meg ezen átállási folyamat során.

Működési szakasz

5. ***Adatok***

A más rendszerekkel elektronikusan kicserélt számítógépes rendszereknek a kockázatok minimalizálása érdekében magukban kell foglalniuk a megfelelő beépített ellenőrzéseket az adatok helyes és biztonságos bevitele és feldolgozása érdekében.

6. ***Pontossági ellenőrzések***

A manuálisan bevitt kritikus adatok esetében az adatok pontosságát további ellenőrzésnek kell alávetni. Ezt az ellenőrzést egy második üzemeltető vagy érvényesített elektronikus eszköz is

elvégezheti. A rendszerbe hibásan vagy helytelenül bevitt adatok kritikusságát és lehetséges következményeit kockázatkezelés keretében kell kezelni.

7. *Az adatok tárolása*

7.1 Az adatokat fizikai és elektronikus eszközökkel egyaránt biztosítani kell kár ellen. Ellenőrizni kell a tárolt adatok hozzáférhetőségét, olvashatóságát és pontosságát. Az adatmegőrzés teljes időtartama alatt biztosítani kell az adatokhoz való hozzáférést.

7.2 Rendszeres biztonsági másolatot kell készíteni minden releváns adatról. A biztonsági másolati adatok integritását és pontosságát, valamint az adatok helyreállításának képességét a validálás során ellenőrizni kell, és rendszeresen ellenőrizni kell.

8. *Kinyomatok*

8.1 Lehetővé kell tenni az elektronikusan tárolt adatok egyértelmű nyomtatott példányainak beszerzését.

8.2 A tételfelszabadítást alátámasztó nyilvántartások esetében lehetővé kell tenni olyan fájlok létrehozását, amelyek jelzik, hogy az eredeti bejegyzés óta az adatok bármelyike megváltozott-e.

9. *Audit trail*

A kockázatértékelés alapján fontolóra kell venni, hogy a rendszerbe beépítsék a GMP-vel kapcsolatos valamennyi változás és törlés nyilvántartását (a létrehozott rendszer „ellenőrzési nyomvonal”). A GMP-re vonatkozó adatok megváltoztatása vagy törlése esetén az indokot dokumentálni kell. Az ellenőrzési nyomvonalnak rendelkezésre kell állnia, általánosan érthető formára konvertálhatónak kell lennie, és azt rendszeresen felül kell vizsgálni.

10. *Változás- és konfigurációmenedzsment*

A számítógépes rendszer bármilyen módosítása, beleértve a rendszerkonfigurációkat is, csak egy meghatározott eljárással összhangban, ellenőrzött módon történhet.

11. *Időszakos értékelés*

A számítógépes rendszereket rendszeres időközönként értékelni kell annak megerősítése érdekében, hogy azok érvényes állapotban maradnak és megfelelnek a helyes gyártási gyakorlatnak. Ezeknek az értékeléseknek adott esetben ki kell terjedniük a funkciók aktuális körére, az eltérési nyilvántartásokra, a váratlan eseményekre, a problémákra, a korábbi frissítésekre, a teljesítményre, a megbízhatóságra, a biztonságra és a validálási állapotjelentésekre.

12. *Biztonság*

12.1 Fizikai és/vagy logikai ellenőrzéseket kell alkalmazni annak érdekében, hogy a számítógépes rendszerhez való hozzáférést az arra jogosult személyekre korlátozzák. A rendszerbe történő jogosulatlan belépés megakadályozására alkalmas módszerek közé tartozhat a kulcsok, belépőkártyák, jelszóval ellátott személyi kódok, biometrikus azonosítók, a számítógépes berendezésekhez és adattároló területekhez való korlátozott hozzáférés.

12.2 A biztonsági ellenőrzések mértéke a számítógépes rendszer kritikusságától függ.

12.3 A hozzáférési engedélyek létrehozását, módosítását és törlését rögzíteni kell.

12.4 Az adatok és dokumentumok kezelésére szolgáló rendszereket úgy kell kialakítani,

hogy azok rögzítsék az adatokat bevivő, megváltoztató, megerősítő vagy törlő gazdasági szereplők személyazonosságát, beleértve a dátumot és az időpontot is.

13. ***Biztonsági események kezelése***

Minden eseményt jelenteni és értékelni kell, nem csak a rendszerhibákat és az adathibákat. Azonosítani kell a kritikus esemény kiváltó okát, amelynek a korrekciós és megelőző intézkedések alapját kell képeznie.

14. ***Elektronikus aláírás***

Az elektronikus nyilvántartások elektronikusan is aláírhatók. Az elektronikus aláírások várhatóan:

a. ugyanolyan hatásúak, mint a vállalat határain belüli kézzel írott aláírások,
b. állandóan kapcsolódnak a nyilvántartásukhoz,
c. adja meg az alkalmazás időpontját és dátumát.

15. ***Tételfelszabadítás***

Amennyiben számítógépes rendszert használnak a tanúsítás és a tételek felszabadításának nyilvántartására, a rendszernek lehetővé kell tennie, hogy csak a minősített személyek tanúsíthassák a tételek felszabadítását, és egyértelműen azonosítania és rögzítenie kell a tételeket felszabadító vagy tanúsító személyt. Ezt elektronikus aláírással kell elvégezni.

16. ***Az üzletmenet folytonossága***

A kritikus folyamatokat támogató számítógépes rendszerek rendelkezésre állása érdekében rendelkezni kell e folyamatok támogatásának folyamatosságáról rendszerzavar esetén (pl. kézikönyv vagy alternatív rendszer).Az alternatív megoldások alkalmazásához szükséges időnek kockázaton kell alapulnia, és meg kell felelnie egy adott rendszernek és az általa támogatott üzleti folyamatnak. Ezeket az intézkedéseket megfelelően dokumentálni és tesztelni kell.

17. ***Archiválás***

Az adatok archiválhatók. Ezen adatok hozzáférhetőségét, olvashatóságát és sértetlenségét ellenőrizni kell. Ha lényeges változtatásokat kell végrehajtani a rendszerben (pl. számítógépes berendezések vagy programok), biztosítani és tesztelni kell az adatok lehívásának képességét.

Glosszárium

Alkalmazás: Meghatározott platformra/hardverre telepített, meghatározott funkcionalitást biztosító szoftver/hardver

Személyre szabott/személyre szabott számítógépes rendszer: Egy adott üzleti folyamatnak megfelelő, egyedileg kialakított számítógépes rendszer

A polcszoftver forgalmazása: Kereskedelmi forgalomban kapható szoftverek, amelyek használatra való alkalmasságát a felhasználók széles köre igazolja.

Informatikai infrastruktúra: Az alkalmazás működését lehetővé tevő hardver és szoftver, például hálózati szoftver és operációs rendszerek.

Életciklus:A rendszer élettartamának valamennyi szakasza a kezdeti követelményektől a megszüntetésig, beleértve a tervezést, a specifikációt, a programozást, a tesztelést, a telepítést, az üzemeltetést és a karbantartást.

Folyamattulajdonos: Az üzleti folyamatért felelős személy.

Rendszertulajdonos:A számítógépes rendszer rendelkezésre állásáért és karbantartásáért, valamint a rendszerben tárolt adatok biztonságáért felelős személy.

Harmadik fél: Nem közvetlenül a gyártási és/vagy behozatali engedély jogosultja által irányított felek.