EudraLex

Az Európai Unió Gyógyszerszabályozási Előírásai

4. Kötet

A Humán és Állatgyógyászati Felhasználású Gyógyszerek
Helyes Gyógyszergyártási Gyakorlatának
EU Iránymutatásai

11. Melléklet: Számítógépes Rendszerek

A részletes iránymutatások kiadásának jogi alapjai: Az emberi felhasználásra szánt gyógyszerek közösségi kódexéről szóló 2001/83/EK Irányelv 47. cikke, és az állatgyógyászati készítmények uniós kódexéről szóló 2001/82/EK Irányelv 51. cikke. Ez a dokumentum útmutatást nyújt a gyógyszerek helyes gyártási gyakorlat (GMP) elveinek és iránymutatásainak értelmezéséhez, ahogyan az le van fektetve az emberi felhasználásra szánt gyógyszerekről szóló 2003/94/EK Irányelvben, és az állatgyógyászati felhasználású gyógyszerek esetén a 91/412/EEK Irányelvben.

A dokumentum státusza: 1. felülvizsgálat

A változtatások okai: a Melléklet átdolgozásra került a számítógépes rendszerek megnövekedett használata, illetve ezen rendszerek megnövekedett komplexitása miatt. Ennek megfelelően módosításra került a GMP Iránymutatás 4. Fejezete is.

Hatályosság kezdete: 2011. június 30.

Alapelv

Ez a melléklet alkalmazandó a GMP szabályozás alatt álló tevékenységek részeként alkalmazott számítógépes rendszerek minden formájára. Számítógépes rendszer alatt a software-ek és hardware-ek olyan halmazát értjük, melyek együttesen látnak el bizonyos feladatokat.

Az alkalmazásokat validálni kell; az IT infrastruktúrát pedig kvalifikálni kell.

A manuális műveletek számítógépes rendszerrel történő helyettesítése nem eredményezheti a termékminőség, a folyamatkontroll vagy a minőségbiztosítás színvonalának csökkenését. A folyamat összesített kockázata nem emelkedhet.

Általános elvek

1. ***Kockázatkezelés***

A számítógépes rendszer életciklusára kockázatkezelést kell alkalmazni, figyelembe véve a betegbiztonságot, az adatintegritást és a termékminőséget. A kockázatkezelés részeként, a validálás mértékének és az adatintegritási kontrollnak, a számítógépes rendszer igazolt és dokumentált kockázatértékelésén kell alapulnia.

2. ***Személyzet***

Szoros együttműködés szükségeltetik a releváns személyek között, mint pl. a Folyamatgazda, a Rendszergazda, a QP és az IT-részleg. Minden személynek megfelelő végzettségekkel, megfelelő szintű hozzáféréssel és meghatározott felelősségekkel kell rendelkezniük a kiosztott feladataik végrehajtásához.

3. ***Beszállítók és Szolgáltatók***

3.1 Ahol harmadik feleket (pl. beszállítók, szolgáltatók) alkalmaznak a számítógépes rendszerek vagy a kapcsolódó szolgáltatások pl. igénybevételéhez, telepítéséhez, konfigurálásához, integrálásához, validálásához, karbantartásához (pl. távoli hozzáféréssel), módosításához, megőrzéséhez, vagy az adatfeldolgozáshoz, ott kell, hogy legyenek hivatalos egyezmények a gyártó és a harmadik felek között, és ezeknek egyértelműen le kell írniuk a harmadik felek felelősségeit. Az IT-részlegek esetén hasonlóan kell eljárni.

3.2 A beszállító hozzáértése és megbízhatósága kulcsfontosságú egy termék vagy szolgáltató kiválasztásakor. Az audit szükségességét kockázatelemzéssel kell megindokolni.

3.3 A szabadon elérhető termékekhez kapott dokumentumokat felül kell vizsgálnia a szabályozott felhasználónak, a követelmények megfelelőségének megállapításának céljából.

3.4 A beszállítókkal vagy szoftver- és alkalmazott rendszerek fejlesztőivel kapcsolatos minőségügyi rendszer- és audit információkat elérhetővé kell tenni az inspektorok számára, ha kérik.

Projektfázis

4. ***Validálás***

4.1 A validálási dokumentációnak és jelentésnek le kell fednie az életciklus releváns szakaszait. A gyártóknak tudniuk kell igazolniuk az elvárásaikat, protokolljaikat, elfogadási kritériumaikat, eljárásaikat és feljegyzéseiket a kockázatértékelésük alapján.

4.2 A validálási dokumentációnak magába kell foglalnia a változáskövetési feljegyzéseket (ha vannak), és minden a validálás során észlelt eltérést.

4.3 Kell, hogy legyen egy naprakész lista minden releváns rendszerről és a GMP-ben betöltött funkcióikról.

A kritikus rendszerek esetén kell, hogy legyen egy naprakész rendszerleírás, amelyben részletezve vannak a fizikai és logikai intézkedések, az adatáramlás és a más rendszerekkel vagy folyamatokkal való kommunikáció, a hardware és software előfeltételek, és a biztonsági intézkedések.

4.4 A Felhasználói Követelmények Specifikációjának le kell írnia a számítógépes rendszerrel kapcsolatos elvárásokat, továbbá annak dokumentált kockázatértékelésen és a GMP elveken kell alapulnia. A felhasználói követelményeknek nyomon követhetőnek kell lenniük a teljes életciklus során.

4.5 A szabályozott felhasználónak minden észszerű lépést meg kell tennie annak biztosítására, hogy a rendszer fejlesztése egy megfelelő minőségirányítási rendszer szerint történjen. A beszállítót megfelelően értékelni kell.

4.6 A személyre szabott vagy egyedi számítógépes rendszerek validálásához ki kell alakítani egy olyan eljárást, amely biztosítja a minőség és a teljesítménymutatók hivatalos értékelését és jelentését a rendszer életciklusának minden szakaszában.

4.7 A vizsgálati módszerek és vizsgálati forgatókönyvek megfelelőségére vonatkozó bizonyítékokat be kell tudni mutatni. Különösképpen figyelni kell a rendszer/folyamat paraméterek limitjeire, adatlimitekre és hibakezelésre. Az automatizált vizsgálati eszközöknek és vizsgálati környezetnek dokumentált megfelelőségi értékeléssel kell rendelkezniük.

4.8 Az egyik adatformából másik formába való átalakítása vagy másik rendszerbe való továbbítása esetén, a validálásnak ki kell térnie annak az ellenőrzésére, hogy az adatok értéke/jelentése nem változik meg a transzfer során.

Működési fázis

5. ***Adat***

A más rendszerekkel elektronikus adatcserét folytató számítógépes rendszereknek beépített módon ellenőrizniük kell a helyes és biztonságos adatbevitelt és –feldolgozást, a kockázatok csökkentésének érdekében.

6. ***Pontossági Ellenőrzések***

A manuálisan bevitt kritikus adatokat további ellenőrzésnek kell alávetni a pontosságuk ellenőrzésére. Ez az ellenőrzés elvégezhető egy második operátor által, de validált elektronikus úton is. A rendszerbe hibásan vagy helytelenül bevitt adatok kritikusságát és lehetséges következményeit kockázatkezeléssel kell felmérni.

7. ***Adattárolás***

7.1 Az adatokat mind fizikálisan, mind elektronikusan meg kell védeni a károsodástól. A tárolt adatok esetén ellenőrizni kell a hozzáférhetőségüket, olvashatóságukat és pontosságukat. A megőrzés során biztosítottnak kell lennie a hozzáférhetőségnek.

7.2 A releváns adatok rendszeresen biztonsági mentését el kell végezni. A biztonsági mentéssel elmentett adatok integritását, pontosságát és a belőlük történő adatvisszanyerést le kell ellenőrizni a validálás során, illetve rendszeresen monitorozni kell.

8. ***Kinyomtatás***

8.1 Biztosítani kell az elektronikusan tárolt adatok, tiszta, olvasható formában történő kiírathatását.

8.2 A tételfelszabadítást során figyelembe vett feljegyzések esetén biztosítani olyan kiíratások előállítását, melyeken jelölve van az, hogy meg lett-e változtatva bármilyen adat a bevitele óta.

9. ***Audit Trail-ek***

Kockázatértékelés alapján meg kell fontolni a GMP-vel kapcsolatos változtatások és törlések feljegyzésének a rendszerbe történő beépítését. A GMP szempontból releváns adatok megváltoztatásának vagy törlésének okát dokumentálni kell. Az audit trail-eknek elérhetőnek kell lenniük és olvasható formába konvertálhatóaknak, illetve rendszeresen felül kell őket vizsgálni.

10. ***Változtatás és Konfigurációkezelés***

A számítógépes rendszeren, beleértve a rendszerkonfigurációt is, csak kontrollált, irányított módon, meghatározott eljárás szerint lehet változtatást végrehajtani.

11. ***Rendszeres értékelés***

A számítógépes rendszereket rendszeresen értékelni kell validitásuk és GMP megfelelőségük igazolásának céljából. Az ilyen ellenőrzéseknek magukba kell foglalniuk – ahol azok alkalmazhatóak – az alkalmazási körök kiterjedtségét, az eltérések feljegyzéseit, az incidenseket, a problémákat, a frissítési előzményeket, a teljesítményt, a megbízhatóságot, a biztonságosságot és a validálási státuszjelentéseket.

*12. **Biztonság***

12.1 Fizikális és/vagy logikai ellenőrzésekkel kell lekorlátozni a számítógépes rendszerekhez való hozzáférést a jóváhagyott személyekre. A nem jóváhagyott hozzáférések megakadályozására megfelelő módszer lehet a kulcsok, belépőkártyák, azonosítókódok, jelszavak, biometrikus azonosítók használata, illetve a számítógépekhez és adattároló területekhez való korlátozott hozzáférés.

12.2 A biztonsági intézkedések mértékének a számítógépes rendszer kritikusságától kell függenie.

12.3 A hozzáférési jogosultságok létrehozását, megváltoztatását és törlését fel kell jegyezni.

12.4 Az adat- és dokumentumkezelő rendszereket úgy kell kialakítani, hogy azok feljegyezzék az adatbevitelt, -megváltoztatást, -megerősítést vagy törlést végző operátorok nevét, idővel és dátummal ellátva.

*13. **Incidenskezelés***

Minden incidenst – nemcsak a rendszerhibákat és adathibákat – jelenteni kell, és értékelni. A kritikus incidensek gyökérokát meg kell határozni, és ennek kell a helyesbítő és megelőző intézkedések alapját képeznie.

*14. **Elektronikus Aláírás***

Az elektronikus feljegyzések aláírhatóak elektronikusan is. Velük kapcsolatos elvárások:

a. a vállalaton belül egyenértékű legyen a kézi aláírással,
b. ne legyen eltávolítható a feljegyzésről, amelyre vonatkozik,
c. szerepeljen rajta az aláírás ideje és dátuma.

*15. **Tételfelszabadítás***

Ahol számítógépes rendszert használnak tételbizonylatolásra és felszabadításra, ott a rendszer csak a Meghatalmazott Személyek számára engedheti a tételbizonylatolást és felszabadítást, továbbá egyértelműen azonosítania kell a tételbizonylatolást és felszabadítást végző személyt. Elektronikus aláírással kell végezni az elektronikus tételtanúsítást és felszabadítást.

*16. **Folyamatos működtetés***

A kritikus folyamatokat ellátó számítógépes rendszerek folyamatos működtetését biztosítani kell rendszerösszeomlás esetére is, pl. manuális műveletekre vagy egy másik rendszerre való átállással. Az új működtetésre való átállás idejét kockázatértékeléssel kell meghatározni az adott rendszerre és az általa ellátott feladatra nézve. Ezeket az intézkedéseket megfelelően kell dokumentálni és ellenőrizni.

*17. **Archiválás***

Az adatokat lehet archiválni. Viszont ezeket az adatokat ellenőrizni kell hozzáférhetőségre, olvashatóságra és integritásra. Ha a rendszeren jelentős változtatásokat hajtanak végre, akkor biztosítani és ellenőrizni kell az adatok visszanyerhetőségét.

Fogalommeghatározások

Alkalmazás: egy meghatározott hardware-re/platformra telepített software, mely bizonyos feladatot lát el.

Személyre szabott / Egyedi számítógépes rendszer: egy specifikus feladat ellátására egyedileg megtervezett számítógépes rendszer.

Szabadon hozzáférhető software: általánosan elérhető software, mely széleskörű felhasználók között alkalmazható bizonyítottan.

IT Infrastruktúra: Azon számítógépes hálózatok és operációs rendszerek, melyek lehetővé teszik az alkalmazások működését.

Életciklus: A rendszer életének összes fázisa, a kezdeti elvárásoktól a visszavonultatásáig, beleértve a kialakítást, a specifikációkat, programozását, tesztelését, telepítését, működtetését és karbantartását.

Folyamatgazda: A működtetésért felelős személy.

Rendszergazda: A számítógépes rendszer elérhetőségéért, karbantartásáért és a rendszerben tárolt adatok biztonságáért felelős személy.

Harmadik fél: Olyan felek, akik nem a forgalomba hozatali engedélyes/behozatali engedélyes alá tartoznak.