Aneks 11

KOMPJUTERIZOVANI SISTEMI

Princip

Ovaj aneks se odnosi na sve oblike kompjuterizovanih sistema koji se koriste kao dio aktivnosti koje su regulisane Smjernicama dobre proizvođačke prakse.
Kompjuterizovani sistem je skup softverskih i hardverskih komponenata koje zajedno obezbjeđuju određenu funkcionalnost sistema.

Aplikacija treba da bude validirana; IT infrastruktura treba da bude kvalifikovana.

Ukoliko kompjuterizovani sistem zamjenjuje manuelne operacije, njegova upotreba ne treba da dovede do smanjenja kvaliteta proizvoda, kontrole procesa ili obezbjeđenja kvaliteta. Ovi sistemi ne treba da povećavaju ukupan rizik procesa.

Opšte odredbe

1. Upravljanje rizikom

Upravljanje rizikom treba da se primjenjuje tokom cijelog životnog ciklusa kompjuterizovanog sistema uzimajući u obzir bezbjednost pacijenta, integritet podataka i kvalitet proizvoda. Kao dio sistema upravljanja rizikom, odluke o obimu validacije i kontrola integriteta podataka treba da se zasnivaju na opravdanoj i dokumentovanoj procjeni rizika kompjuterizovanog sistema.

2. Osoblje

Treba da postoji bliska saradnja između relevantnog osoblja kao što su Vlasnik procesa, Vlasnik sistema, Kvalifikovana lica i osoblje zaduženo za kompjuterizovane sisteme (*IT* osoblje). Svo osoblje treba da ima odgovarajuće kvalifikacije, nivo pristupa i definisane odgovornosti za obavljanje svojih zadataka.

3. Dobavljači i davaoci usluga

3.1 Kada se koriste treće strane (npr. dobavljači, davaoci usluga) da npr. obezbijede, instaliraju, konfigurišu, integrišu, validiraju, održavaju (npr. preko udaljenog pristupa), modifikuju ili čuvaju kompjuterizovane sisteme ili povezane usluge ili za obradu podataka, mora da postoji zaključen ugovor između proizvođača i bilo koje treće strane, kojim su jasno definisane odgovornosti treće strane. Analogno, treba da se razmotre odjeljenja koja će se baviti informacionim tehnologijama (IT odjeljenja).

3.2 Kompetentnost i pouzdanost dobavljača su ključni faktori pri izboru davaoca roba ili usluga. Potreba za njihovom provjerom (*audit*), treba da bude zasnovana na procjeni rizika.

3.3 Dokumentacija dostavljena sa standardnim komercijalnim softverskim (*off-the-shelf*) proizvodima treba da bude pregledana od strane ovlašćenih korisnika koji provjeravaju da li su ispunjeni korisnički zahtjevi.

3.4 Informacije o sistemu kvaliteta i provjeri (*audit*) trećih strana koje razvijaju ili isporučuju softver i implementirani sistemi treba da budu dostupni inspektorima na njihov zahtjev.

Projektna faza

4. Validacija

4.1 Dokumentacija o validaciji i izveštaji treba da obuhvate relevantne korake životnog ciklusa. Proizvođači treba da budu sposobni da opravdaju standarde, protokole, kriterijume prihvatljivosti, procedure i zapise zasnovane na njihovoj procjeni rizika.

4.2 Dokumentacija o validaciji treba da obuhvati zapise o kontroli izmjena (ako je primjenjivo) i zapise o svim odstupanjima koja su zabilježena tokom procesa validacije.

4.3 Ažurirana lista sa podacima o svim relevantnim sistemima i njihovoj *GMP* funkcionalnosti (inventar) treba da bude dostupna.
Za kritične sisteme treba da bude dostupan ažuriran opis sistema koji detaljno opisuje fizičku i logičku strukturu, protok podataka i interfejse sa drugim sistemima ili procesima, bilo koji hardverski ili softverski preduslov i mjere bezbjednosti.

4.4 Specifikacije zahtjeva korisnika treba da opišu potrebnu funkciju kompjuterizovanog sistema i da se zasnivaju na dokumentovanoj procjeni rizika i *GMP* uticaju. Korisnički zahtjevi treba da budu sljedljivi tokom cijelog životnog ciklusa.

4.5 Ovlašćeni korisnik treba da preduzme sve razumne korake, da obezbijedi da sistem bude razvijen u skladu sa odgovarajućim sistemom upravljanja kvalitetom. Treba da se izvrši procjena dobavljača na odgovarajući način.

4.6 Za validaciju posebno dizajniranih (*bespoke*) ili prilagođenih (*customized*) kompjuterizovanih sistema treba da postoji ustanovljen proces koji omogućava formalnu procjenu i izveštavanje o mjerama vezanim za kvalitet i performanse svih faza životnog ciklusa sistema.

4.7 Dokaz o odgovarajućim metodama i postupcima testiranja treba da postoji. Naročito treba da se razmotre limiti parametara sistema (procesa), limiti podataka i postupanje u slučaju greške. Za automatizovane alate za testiranje i uslove testiranja treba da postoji dokumentovana procjena njihove adekvatnosti.

4.8 Ako se podaci prenose u drugi format podataka ili sistem, validacija treba da uključi provjere da nijesu promjenjene vrijednosti i/ili značenje podataka tokom ovog procesa prenosa.

Operativna faza

5. Podaci

Kompjuterizovani sistemi koji elektronski razmijenjuju podatke sa drugim sistemima treba da imaju ugrađene odgovarajuće provjere za pravilan i bezbjedan unos i obradu podataka, da bi minimizirali rizike.

6. Provjera tačnosti

Za kritične podatke koji se unose ručno, treba dodatno da se provjeri tačnost podataka. Ovu provjeru može da izvrši drugi operater ili se ona može obaviti validiranim elektronskim sredstvima.
Kritičnost i potencijalne posljedice pogrešnih ili neispravno unijetih podataka u sistem treba da budu obuhvaćeni upravljanjem rizikom.

7. Čuvanje podataka

7.1 Podaci treba da budu obezbjeđeni od oštećenja, kako fizičkim tako i elektronskim sredstvima. Treba da se provjeri dostupnost, čitljivost i tačnost sačuvanih podataka. Pristup podacima treba da bude obezbjeđen tokom perioda čuvanja.

7.2 Treba da se obezbijede redovne rezervne kopije (*back-up*) svih relevantnih podataka. Integritet i tačnost rezervnih kopija i mogućnost za vraćanje (*restore*) podataka treba da se provjere tokom validacije, kao i da se periodično provjere.

8. Štampani izveštaji

8.1 Treba da se omogući dobijanje čitkih štampanih kopija elektronski sačuvanih podataka.

8.2 Za zapise koji podržavaju puštanje serije lijeka u promet, treba da postoji mogućnost da se generišu štampani izvještaji koji ukazuju na to da li je neki od podataka promijenjen u odnosu na prvobitni unos.

9. Audit trails

Na osnovu procjene rizika treba da se razmotri da sistem generiše zapise o svim *GMP* relevantnim promjenama i brisanju (sistemski generisan *audit trail*). Razlog za promjenu ili brisanje *GMP* relevantnih podataka treba da bude dokumentovan.
Audit trails treba da budu raspoloživi i da mogu da se konvertuju u razumljiv oblik i da se redovno pregledaju.

10. Izmjene i upravljanje konfiguracijom

Bilo kakve izmjene u kompjuterizovanom sistemu, uključujući konfiguracije sistema, mogu da se vrše samo na kontrolisan način u skladu sa definisanom procedurom.

11. Periodična procjena

Kompjuterizovani sistemi treba periodično da se procjenjuju, kako bi se potvrdio njihov validacioni status, kao i usaglašenost sa Dobrom proizvođačkom praksom. Kada je primjenljivo, ovakve procjene treba da uključe trenutni obim funkcionalnosti, zapise o odstupanjima, incidente, probleme, istoriju ažuriranja (*upgrade*), performanse, pouzdanost, bezbjednost i izvještaje o validacionom statusu.

12. Bezbjednost

12.1 Fizičke i/ili logičke kontrole treba da budu u funkciji kako bi se pristup kompjuterizovanom sistemu ograničio na ovlašćena lica. Odgovarajuće metode sprečavanja neovlašćenog ulaska u sistem mogu da uključe upotrebu hardverskih "ključeva", pristupnih kartica, ličnih šifri sa lozinkama, biometrijskih podataka, ograničen pristup računarskoj opremi i prostoru za čuvanje podataka.

12.2 Stepen bezbjednosnih kontrola zavisi od kritičnosti kompjuterizovanog sistema.

12.3. Kreiranje, promjena i ukidanje ovlašćenja za pristup, treba da budu zabilježeni.

12.4. Sistemi za upravljanje podacima i dokumentima treba da budu dizajnirani tako da bilježe identitet operatora koji unose, mijenjaju, potvrđuju ili brišu podatke uključujući datum i vrijeme.

13. Upravljanje incidentima

Svi incidentni slučajevi, a ne samo otkazivanja sistema i greške u podacima, treba da budu prijavljene i procijenjene. Osnovni uzrok kritičnog incidenta treba da bude identifikovan i da bude osnova za korektivne i preventivne aktivnosti.

14. Elektronski potpis

Elektronski zapisi mogu biti potpisani elektronski. Od elektronskog potpisa se očekuje da:

a. Ima isti značaj kao i svojeručni potpisi unutar kompanije,
b. Bude trajno povezan sa odgovarajućim zapisom,
c. Uključuje vrijeme i datum kada su primjenjeni.

15. Puštanje serije lijeka u promet

Kada se kompjuterizovani sistem koristi za izdavanje sertifikata i puštanje serije lijeka u promet, sistem treba da dozvoli samo Kvalifikovanim licima da odobre puštanje serije lijeka u promet i jasno da identifikuje i evidentira osobu koja izdaje sertifikat i pušta seriju lijeka u promet. Ovaj postupak treba da se izvrši upotrebom elektronskog potpisa.

16. Kontinuitet poslovanja

Za dostupnost kompjuterizovanih sistema koji podržavaju kritične procese, treba da se primjenjuju mjere kako bi se obezbjedio kontinuitet podrške za te procese u slučaju pada sistema (npr. manuelni ili alternativni sistem). Vrijeme potrebno za aktiviranje alternativnih sistema treba da bude zasnovano na procjeni rizika u odnosu na određeni sistem i poslovni proces koji podržava. Ovi alternativni sistemi treba da se adekvatno dokumentuju i testiraju.

17. Arhiviranje

Podaci se mogu arhivirati. Za arhivirane podatke treba da se provjeri dostupnost, čitljivost i integritet. U slučaju kada su izvršene značajne promjene u sistemu (npr. računarska oprema ili programi), treba da se osigura i testira sposobnost preuzimanja arhiviranih podataka.

Rječnik

Aplikacija*:* Softver instaliran na definisanoj platformi/hardveru koji pruža specifičnu funkcionalnost.

Vlasnik procesa: lice odgovorno za poslovni proces.

Vlasnik sistema: Osoba odgovorna za dostupnost i održavanje kompjuterizovanog sistema i za bezbjednost podataka koji se nalaze u tom sistemu.

Životni ciklus: Sve faze u životu sistema od početnih zahtjeva do povlačenja uključujući dizajn, specifikaciju, programiranje, testiranje, instalaciju, rad i održavanje.

IT infrastruktura: Hardver i softver, kao što su softver za umrežavanje i rad sistema, što omogućava da aplikacija funkcioniše.

Posebno dizajniran (*bespoke*) / prilagođen (*customized*) kompjuterizovani sistem: kompjuterizovani sistem koji je individualno dizajniran da odgovara određenom poslovnom procesu.

Standardni komercijalni softver: Komercijalno dostupan softver, čija je pogodnost za upotrebu demonstrirana širokim spektrom korisnika.

Treća strana: Strane kojim ne upravlja direktno nosilac dozvole za proizvodnju i/ili uvoz.