BIJLAGE 11:

GEAUTOMATISEERDE SYSTEMEN

Beginsel

Deze bijlage is van toepassing op alle soorten geautomatiseerde systemen gebruikt als onderdeel van GMP gereguleerde activiteiten. Een geautomatiseerd systeem omvat een combinatie van software- en hardwarecomponenten die samen bepaalde functionaliteiten vervullen.

De applicatie/toepassing dient te worden gevalideerd en IT-infrastructuur dient te worden gekwalificeerd.

Wanneer een geautomatiseerd systeem een handmatige bewerking vervangt, mag dit niet leiden tot een afname van de kwaliteit van het product, de controle over het proces of de kwaliteitsborging. Er mag geen sprake zijn van verhoging van het globale risico van het proces.

Algemeen

1. ***Risicobeheer***

Risicobeheer dient te worden toegepast gedurende de gehele levenscyclus van het geautomatiseerde systeem, rekening houdend met de veiligheid van de patiënt, de integriteit van de gegevens en de kwaliteit van het product. Beslissingen over de omvang van validatie en integriteitscontroles van gegevens in het kader van een risicobeheersysteem dienen te worden gebaseerd op een gerechtvaardigde en gedocumenteerde risicobeoordeling van het geautomatiseerde systeem.

2. ***Personeel***

Er dient een nauwe samenwerking te zijn tussen alle relevante personeelsleden, zoals de proceseigenaar, de systeemeigenaar, bevoegde personen en IT-personeel. Alle personeelsleden dienen over de geschikte kwalificaties en passende toegangen te beschikken, en vastgestelde verantwoordelijkheden te hebben om de hen toegewezen taken uit te voeren.

3. ***Leveranciers en dienstverleners***

3.1 Wanneer derden (bijvoorbeeld leveranciers of dienstverleners) worden gebruikt om bijvoorbeeld een geautomatiseerd systeem of aanverwante dienst te leveren, te installeren, te configureren, te integreren, te valideren, te onderhouden (bijv. via toegang op afstand), te wijzigen of te bewaren of om gegevens te verwerken, dient er sprake te zijn van formele overeenkomsten tussen de fabrikant en alle derde partijen en dient in deze overeenkomsten duidelijk de verantwoordelijkheden van de derde partij te zijn vermeld. IT-afdelingen dienen analoog te worden beschouwd.

3.2 De deskundigheid en betrouwbaarheid van een leverancier zijn sleutelfactoren bij het selecteren van een product of dienstverlener. De noodzaak voor een audit dient te worden gebaseerd op basis van een risicobeoordeling.

3.3 De documentatie die bij commerciële in de handel verkrijgbare producten wordt geleverd dient aandachtig te worden geëvalueerd door de gebruikers onderworpen aan de farmaceutische wetgeving, om na te gaan of deze aan de gebruiksvereisten voldoen.

3.4 Informatie inzake het kwaliteitssysteem en audits in verband met leveranciers of ontwikkelaars van software en de geïnstalleerde systemen dient op verzoek ter beschikking te worden gesteld aan de inspecteurs.

Projectfase

4. ***Validatie***

4.1 De documentatie en verslagen inzake de validatie dienen de relevante fasen van de levenscyclus te omvatten. De fabrikanten dienen in staat te zijn om hun normen, protocollen, aanvaardingscriteria, procedures en documenten te rechtvaardigen op basis van hun risicobeoordeling.

4.2 Validatiedocumentatie dient de registraties van de controle op wijzigingen te omvatten (indien van toepassing), alsook rapporten van alle afwijkingen die tijdens het validatieproces zijn waargenomen.

4.3 Er dient een actuele lijst (inventaris) van alle betrokken systemen en hun GMP functie beschikbaar te zijn.

Voor kritische systemen dient een actuele beschrijving van het systeem beschikbaar te zijn, waarin de fysieke en logische indeling, de gegevensstromen en interfaces met andere systemen of processen, de hardware- en softwarebenodigdheden en veiligheidsmaatregelen zijn uiteengezet.

4.4 In specificaties inzake gebruikersvereisten (« User Requirements Specifications » - URS) dienen de vereiste functies van het geautomatiseerd systeem te zijn beschreven. Deze dienen gebaseerd te zijn op een gedocumenteerde risicobeoordeling en de GMP-impact. Gebruikersvereisten dienen traceerbaar te zijn gedurende de gehele levenscyclus.

4.5 De gebruiker, onderworpen aan de farmaceutische regelgeving, neemt alle redelijke maatregelen om ervoor te zorgen dat het systeem is ontwikkeld in overeenstemming met een passend kwaliteitsbeheersysteem. De leverancier dient dienovereenkomstig te worden beoordeeld.

4.6 Voor de validatie van op maat gemaakte of gepersonaliseerde geautomatiseerde systemen dient een werkwijze beschikbaar te zijn waarmee wordt gezorgd voor een formele beoordeling en verslag van kwaliteits- en prestatiemaatregelen voor alle fasen in de levenscyclus van het systeem.

4.7 De geschiktheid van testmethoden en -scenario’s dient te worden aangetoond. Er dient in het bijzonder rekening te worden gehouden met de parameterlimieten van het systeem (proces) en de gegevens, alsook met de omgang met fouten. Voor geautomatiseerde testinstrumenten en testomgevingen dienen gedocumenteerde geschiktheidsbeoordelingen beschikbaar te zijn.

4.8 Indien gegevens worden omgezet naar een ander bestandsformaat of naar een ander systeem dient bij de validatie te worden gecontroleerd of de gegevens tijdens de omzetting

niet zijn gewijzigd, qua waarden of qua betekenis.

Operationele fase

5. *Gegevens*

Geautomatiseerde systemen voor de elektronische uitwisseling van gegevens met andere systemen dienen passende ingebouwde controles voor de correcte en veilige invoer en verwerking van gegevens te bevatten, om de risico's tot een minimum te beperken.

6. *Nauwkeurigheidscontroles*

Wanneer kritische gegevens handmatig worden ingevoerd, dient er een bijkomende controle op de juistheid van de gegevens plaats te vinden. Deze controle kan worden uitgevoerd door een tweede operator of via gevalideerde elektronische middelen. De mate van kriticaliteit en de mogelijke gevolgen van verkeerde of onjuist ingevulde gegevens dienen te vallen onder een systeem van risicobeheer.

7. *Opslag van gegevens*

7.1 Gegevens dienen zowel fysiek als elektronisch te worden beveiligd tegen schade. Opgeslagen gegevens dienen te worden gecontroleerd op toegankelijkheid, leesbaarheid en correctheid. De toegang tot gegevens dient te worden gewaarborgd tijdens de bewaarperiode.

7.2 Er dienen regelmatig back-ups van alle relevante gegevens te worden uitgevoerd. De integriteit en juistheid van back-upgegevens en het vermogen om de gegevens terug te zetten dienen tijdens de validatie te worden gecontroleerd en periodiek te worden gecontroleerd.

8. *Afdrukken*

8.1 Het dient mogelijk te zijn om duidelijk gedrukte kopieën van elektronisch opgeslagen gegevens te verkrijgen.

8.2 Voor gegevens, noodzakelijk voor de vrijgave van partijen dient het mogelijk te zijn afdrukken te maken waarop is vermeld of de gegevens sinds de eerste invoer werden gewijzigd.

9. *Traceerbaarheid van wijzigingen (Audit Trails)*

Er dient te worden overwogen om op basis van een risicobeoordeling een register van alle GMP relevante wijzigingen en verwijderingen (een door het systeem gegenereerde audit trail) in het systeem in te bouwen. Voor het wijzigen of verwijderen van GMP relevante gegevens dient de reden te worden gedocumenteerd. Audit trails dienen beschikbaar te zijn en dienen te kunnen worden omgezet in een algemeen begrijpelijke vorm en dienen periodiek te worden herzien.

10. *Wijzigings- en configuratiebeheer*

Elke wijziging aan een geautomatiseerd systeem met inbegrip van de systeemconfiguraties dient alleen te worden uitgevoerd op een gecontroleerde manier en overeenkomstig een vastgelegde procedure.

11. ***Periodieke evaluatie***

Geautomatiseerde systemen dienen periodiek te worden geëvalueerd om te bevestigen dat zij gevalideerd en in overeenstemming met GMP blijven. Dergelijke evaluaties dienen, waar nodig, verslagen over de huidige functionaliteiten, registraties van afwijkingen, incidenten, problemen, de geschiedenis van upgrades, performantie, betrouwbaarheid, veiligheid en de validatiestatusrapporten te omvatten.

12. ***Veiligheid***

12.1 Er dienen fysieke en/of logische controles te zijn om de toegang van onbevoegden tot geautomatiseerde systemen te beperken. Gepaste methoden ter preventie van ongeoorloofde toegang tot het systeem kunnen omvatten, het gebruik van sleutels, pasjes, persoonlijke codes met wachtwoorden, biometrische gegevens en beperkte toegang tot de computeruitrusting en de zones voor gegevensopslag.

12.2 De mate van de veiligheidscontroles hangt af van de kritieke aard van het geautomatiseerd systeem.

12.3 Het creëren, wijzigen en intrekken van toegangsrechten dient te worden geregistreerd.

12.4 Systemen voor het beheer van gegevens en documenten dienen zo te worden ontworpen dat de identiteit van operatoren die gegevens invoeren, wijzigen, bevestigen of verwijderen, wordt geregistreerd, met inbegrip van de datum en tijd.

13. ***Incidentenbeheer***

Alle incidenten, niet alleen systeem- en gegevensfouten, dienen te worden geregistreerd en beoordeeld. De oorzaak van een kritisch incident dient te worden geïdentificeerd en dient aan de basis te liggen van correctieve- en preventieve acties.

14. ***Elektronische handtekening***

Elektronische registers kunnen elektronisch worden ondertekend. Elektronische handtekeningen moeten:

a. dezelfde waarde hebben als handgeschreven handtekeningen binnen de grenzen van de onderneming;
b. permanent zijn gekoppeld aan de documenten waar ze betrekking op hebben;
c. de datum en het tijdstip waarop zij zijn gezet, bevatten.

15. ***Vrijgave van partijen***

Wanneer een geautomatiseerd systeem wordt gebruikt voor de registratie van de certificering en de vrijgave van partijen, mogen alleen de bevoegde personen toestemming hebben om de vrijgave van de partijen te certificeren en dient de persoon die de partijen vrijgeeft of certificeert duidelijk te zijn aangeven. Dit dient te worden uitgevoerd met behulp van een elektronische handtekening.

16. ***Bedrijfscontinuïteit***

Er dienen voorzieningen vastgesteld te zijn voor de beschikbaarheid van geautomatiseerde systemen ter ondersteuning van kritische processen om te zorgen voor de continuïteit van

de ondersteuning van deze processen in het geval van storing van het systeem (bv. een handboek of een alternatief systeem). De tijd die nodig is om alternatieve regelingen in gebruik te nemen, dient risico-gebaseerd te zijn en geschikt te zijn voor een bepaald systeem en het proces dat ermee wordt ondersteund. Deze alternatieve regelingen dienen naar behoren te worden gedocumenteerd en getest.

17. ***Archivering***

Data kan worden gearchiveerd. Deze data dient te worden gecontroleerd op toegankelijkheid, leesbaarheid en integriteit. Indien relevante wijzigingen worden aangebracht aan het systeem (bv. computerapparatuur of -programma's), dienen de mogelijkheden voor het oproepen van gegevens worden gewaarborgd en getest.

Glossarium

Applicatie: op een bepaald platform of bepaalde hardware geïnstalleerde software met een specifieke functionaliteit.

Op maat gemaakt of gepersonaliseerd geautomatiseerd systeem: een geautomatiseerd systeem dat apart is ontworpen voor een specifiek bedrijfsproces.

Commerciële kant-en-klare software: in de handel verkrijgbare software, waarvan de geschiktheid voor gebruik is aangetoond door een breed scala van gebruikers.

IT-infrastructuur: hardware en software, zoals netwerksoftware en besturingssystemen die het functioneren van de applicatie mogelijk maken.

Levenscyclus: alle fasen in de levensduur van het systeem, van de oorspronkelijke eisen tot de buitendienststelling, met inbegrip van ontwerp, specificatie, programmering, testen, installatie, werking en onderhoud.

Proceseigenaar: persoon die verantwoordelijk is voor het bedrijfsproces.

Systeemeigenaar: persoon die verantwoordelijk is voor de beschikbaarheid en het onderhoud van een computersysteem en voor de beveiliging van de gegevens die zich op het systeem bevinden.

Derde partij: partijen die niet rechtstreeks onder de verantwoordelijkheid vallen van houder van de fabricage- en/of invoervergunning.