# GMP-Z Annex 11 – Geautomatiseerde systemen

| GMP item | Gewijzigd richtsnoer GMP-Z | Toelichting |
|---|---|---|
| **Principle** | | |
| This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.<br>The application should be validated; IT infrastructure should be qualified.<br>Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process. | GMP | |
| **1 Risk management** | | |
| 1 1. Risk Management<br>Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system. | GMP | |
| **2 Personnel** | | |
| 2. Personnel<br>There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties. | GMP | De GMP geldt, met dien verstande dat in de ziekenhuisapotheek meestal geen Qualified Person in de formele zin, aanwezig is maar wel voor vrijgifte bevoegde personen.<br>De verantwoordelijkheid voor geschikte en gedocumenteerde kwalificaties van ICT personeel dat niet in de apotheek werkzaam is dient in een overeenkomst met de desbetreffende afdeling (bijv ICT-afdeling) geregeld te zijn (zie ook 3.1). |

| **3 Suppliers and Service Providers** | | |
|---|---|---|
| 3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous. | GMP | |
| 3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment. | GMP | |
| 3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled. | GMP | |
| 3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request. | GMP | |
| **4 Validation** | | |
| 4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment. | GMP | |
| 4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process. | GMP | |
| 4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be | GMP | |

| | | |
|---|---|---|
| available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. | | |
| 4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle. | GMP | |
| 4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately | GMP | |
| 4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system. | 4.6-Z<br>Bij op maat gemaakte systemen dienen afspraken gemaakt te worden met de leverancier dat het ontwerp en de bouw van het systeem valideerbaar zijn.<br>Software die door een grote groep ziekenhuizen wordt gebruikt, kan worden beschouwd als ‘commercial of the shelf software’ (zie definities). Deze ondergaat deels centraal een validatie, deels dient er lokaal een validatie plaats te vinden. | Systemen die op maat zijn gemaakt zouden in categorie GAMP 5 vallen. Vaak zal in de ziekenhuisapotheek niet zelf een nieuw systeem gemaakt worden, maar wordt dit door een leverancier uitgevoerd. In die gevallen moet de apotheker afspraken maken met de leverancier dat die ontwikkelfase van het proces voor een auditor inzichtelijk is. |
| 4.7 Evidence of appropriate test methods and test scenarios should be demonstrated.<br>Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy. | GMP | |
| 4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this | GMP | - |

| | | |
|---|---|---|
| migration process. | | |
| **5 Data** | | - |
| Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | GMP | |
| **6 Accuracy Checks** | | |
| For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management. | GMP | |
| **7 Data Storage** | | - |
| Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | GMP | |
| Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically. | GMP | |
| **8 Printouts** | | |
| 8.1 It should be possible to obtain clear printed copies of electronically stored data. | GMP | - |
| 8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry. | GMP | |

| | | |
|---|---|---|
| **9 Audit trails** | | |
| Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed. | 9-Z<br>Een formele audit trail van de geautomatiseerde systemen is binnen de ziekenhuisfarmacie niet in alle gevallen aanwezig. Wel zijn er waarborgen dat alleen bepaalde functionarissen geautoriseerd zijn voor de toegang tot het systeem. | Met autorisatieniveaus is het mogelijk om te achterhalen wie in het systeem iets heeft uitgevoerd en of de persoon daartoe bevoegd was. De statuswijziging van een document, product of grondstof bijvoorbeeld mag alleen door bepaalde functionarissen worden uitgevoerd. |
| **10. Change and Configuration Management** | | |
| Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure | GMP | |
| **11. Periodic evaluation** | | |
| Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports. | GMP | Bij een update van het systeem of bij afwijkingen is het gebruikelijk om na te gaan of het systeem nog steeds aan de eisen voldoet. Daarnaast is het ook nodig periodiek te evalueren, om te voorkomen dat afwijkingen die niet zijn opgemerkt ertoe hebben geleid dat het systeem niet meer aan de eisen voldoet. Dit betekent echter niet dat elk evaluatiemoment een volledige hervalidatie met zich meebrengt. |
| **12. Security** | | |
| 12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | GMP | |
| 12.2 The extent of security controls depends on the criticality of the computerised system. | GMP | |

| | | |
|---|---|---|
| 12.3 Creation, change, and cancellation of access authorisations should be recorded | GMP | |
| 12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time. | GMP | |
| **13. Incident Management** | | |
| All incidents, not only system failures and data errors, should be reported and assessed.<br>The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions. | GMP | . |
| **14. Electronic Signature** | | |
| Electronic records may be signed electronically. Electronic signatures are expected to:<br>a. have the same impact as hand-written signatures within the boundaries of the company,<br>b. be permanently linked to their respective record,<br>c. include the time and date that they were applied. | GMP | |
| **15. Batch release** | | |
| When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature. | GMP | De GMP geldt, met dien verstande dat in de ziekenhuisapotheek meestal geen Qualified Person in de formele zin, aanwezig is maar wel voor vrijgifte bevoegde personen. |
| **16. Business Continuity** | | |
| For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it | GMP | |

| | | |
|---|---|---|
| supports. These arrangements should be adequately documented and tested. | | |
| **17. Archiving** | | |
| Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | GMP | |