DATA INTEGRITY AND DATA SECURITY

ROADMAP FOR EFFECTIVE COMPUTER SYSTEMS VALIDATION

MARCH 30, 2017

PRESENTED BY: LAURENT SAUGRIN
Sr. Computer Validation Specialist, IT Compliance
Laurent.saugrin@dexcom.com
CHAPTER 1: DEFINITIONS

1.1. Data / Raw Data
1.2. Data Integrity
1.3. Data Security

CHAPTER 2: IN-SCOPE / OUT-OF-SCOPE

2.1. Data in Scope / Out-of-Scope
2.2. Computer Systems in Scope / Out-Of-Scope
AGENDA

CHAPTER 3: 21 CFR PART 11. *(Interactive Session – Bonus Material)*

3.1. Some Definitions
3.2. Data Security Related Requirements
3.3. How to Interpret these Requirements?
3.4. Proposed Verification Tests for these Requirements

CHAPTER 4: SECURITY CONSIDERATIONS FOR HOSTED DATA

In-House Hosted Data Vs Externally Hosted Data (Cloud hosted at 3rd party). - Data Security Policy *(Bonus Material)*
CHAPTER 5: COMPUTER SYSTEM VALIDATION

5.1 Overview: V-Model (most commonly used).

5.2 Overview of GAMP 5 Computer System Categories and Applicable Validation Deliverables/Executables
1.1. DATA & RAW DATA

**Data**: Computer data is information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data.”

**Raw Data**: Data that has not been processed for use. A distinction is sometimes made between data and information to the effect that information is the end product of data processing.
Raw data exists in many computerized systems and should be identified during the initial impact or validation determination statement. Examples:

- Quality critical process data from instruments stored within data historian
- Error messages from automation systems
- Event logs and audit trails
- Laboratory instrument data

Does verification of integrity / security, within the scope of Computer System Validation, apply to data or raw data?
1.2. DATA INTEGRITY

MHRA (Medicines and Healthcare Products Regulatory Agency): “The extent to which all data are complete, consistent and accurate throughout data lifecycle”

FDA: “the completeness, consistency and accuracy of data”.
Complete, consistent, and accurate data should be:

- **Attributable,**
- **Legible,**
- **Contemporaneously recorded,**
- **Original or a true copy,** and
- **Accurate.”**

(ALCOA)
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>211.101(d)</td>
<td>Charge-in of components</td>
</tr>
<tr>
<td></td>
<td>211.122</td>
<td>Materials examination and usage criteria</td>
</tr>
<tr>
<td></td>
<td>211.186</td>
<td>Master production and control records</td>
</tr>
<tr>
<td></td>
<td>211.188(b)(11)</td>
<td>Batch production and control records</td>
</tr>
<tr>
<td></td>
<td>212.50(c)(10)</td>
<td>What production and process controls must I have</td>
</tr>
<tr>
<td>L</td>
<td>211.180(e)</td>
<td>General requirements</td>
</tr>
<tr>
<td></td>
<td>212.110(b)</td>
<td>How must I maintain records of my production of PET drugs</td>
</tr>
<tr>
<td>C</td>
<td>211.100(b)</td>
<td>Written procedures; deviations</td>
</tr>
<tr>
<td></td>
<td>211.160(a)</td>
<td>General requirements</td>
</tr>
<tr>
<td>O</td>
<td>211.180</td>
<td>General requirements</td>
</tr>
<tr>
<td></td>
<td>211.194(a)</td>
<td>Laboratory records</td>
</tr>
<tr>
<td>A</td>
<td>211.22(a)</td>
<td>Responsibilities of quality control unit</td>
</tr>
<tr>
<td></td>
<td>211.68</td>
<td>Automatic, mechanic, and electrical equipment</td>
</tr>
<tr>
<td></td>
<td>211.188(b)(11)</td>
<td>Batch production and control records</td>
</tr>
<tr>
<td></td>
<td>212.60(g)</td>
<td>What requirements apply to the laboratories where I test components, in-process materials, and finished PET drug products</td>
</tr>
</tbody>
</table>
REMEMBER: Verifying the integrity of your data means verifying that your data is:

- RELIABLE,
- CONSISTENT, AND
- ACCURATE
1.3. DATA SECURITY

Within the scope of Computer System Validation, Data Security is best defined as the act of protecting data against unauthorized access or corruption.

Typically, not enough controls around computerized systems is the root cause of data security issues.
Data Integrity Vs Data Security:

- Related terms, each playing an important role in the successful achievement of the other
- Data Security is necessary to ensure Data Integrity
- Data Integrity is a desired result of Data Security

Data Integrity refers to the validity and accuracy of data rather than the act of protecting data.
Data Governance Components (non exhaustive): Sum of all measures taken to assure data integrity.

All part of, and defined in your Quality Management Program
2.1. DATA IN SCOPE / OUT-OF-SCOPE

- In Scope:
  - Data that is computer generated, managed, maintained and/or stored in GxP-related computer systems.
  - When generated to satisfy a cGMP requirement, the data becomes a cGMP record. As data is computer data (in our scope), it is therefore defined as an e-record, in accordance with the definition of 21 CFR PART 11.
✓ Data from the device itself (as applicable, and not limited to):

- Readings
- Error Messages, Alarms...
- Device Identification (e.g. serial number, version)

✓ Patient Data: Personal information collected and stored
✓ **Company Data:**
  - Quality: SOPs, Training Records…
  - Testing Results
  - Validation Deliverables
  - Batch Records (or equivalent)

✓ **Complaint Data:**
  - Patients,
  - Professionals (e.g. Doctors)
Out-Of-Scope

- Paper records (GxP records or not)
- Non GxP electronic records (e.g. employee records such as signed contract; information pulled out from GxP records and used for reports, presentations…)
- Company’s financial data
2.2. COMPUTER SYSTEMS IN SCOPE / OUT-OF-SCOPE

- **In Scope:**
  - ✓ GxP computer systems: Software, Enterprise applications, SaaS, Excel spreadsheets…Interface tools (as applicable).
  - ✓ Infrastructure?

  Yes!
Out-Of-Scope:

- Non GxP computer systems
- Device software (as applicable)
- Applications regulated by Sarbanes-Oxley Act (SOX)
3.1 SOME DEFINITIONS

- Closed System: An environment in which system access is controlled by persons who are responsible for the content of electronic records on the system.

- Computerized System: A computerized system is any combination of hardware, software and associated infrastructure, that collects, creates, modifies, maintains, archives, retrieves, or transmits electronic data.
Electronic Records – Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. For the purposes of this presentation, this term is limited to GxP-related records.

Open System – An environment in which system access is not controlled by persons who are responsible for the content of electronic records on the system.
### 3.2 – 3.4. DATA SECURITY RELATED REQUIREMENTS

<table>
<thead>
<tr>
<th>SECTION #</th>
<th>REQUIREMENT DEFINITION</th>
<th>INTERPRETATION</th>
<th>TESTING STRATEGY</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.10(a)</td>
<td>Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</td>
<td>The system must be validated “to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records”.</td>
<td>Make sure that the system validation covers all of the system abilities that are listed in the statement.</td>
</tr>
<tr>
<td>11.10(c)</td>
<td>Protection of records to enable their accurate and ready retrieval throughout the records retention period.</td>
<td>The system shall provide the capability to restrict access by users to the data files or database records to prevent inadvertent or intentional modification or deletion of data files.</td>
<td>This is best verified by thorough testing of role-based security and access permissions to verify that persons cannot alter or delete records.</td>
</tr>
</tbody>
</table>
| 11.10(d)  | Limiting system access to authorized individuals.                                        | 1) The system must use user identification and authorization to restrict access.  
2) The system should have a time-out feature to automatically close or lock user sessions after a configurable period of inactivity.  
3) The system shall permit an administrator to categorize users into specific user groups and define separate security and access privileges for each group. | 1) Verify that system access is restricted to only those individuals who have logon accounts on the system. Do positive and negative testing.  
2) Verify that the system has an inactivity timer that will lock a user session after a set period of inactivity.  
3) Verify that the system provides role-based access control. |
<table>
<thead>
<tr>
<th>SECTION #</th>
<th>REQUIREMENT DEFINITION</th>
<th>INTERPRETATION</th>
<th>TESTING STRATEGY</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.10(e)</td>
<td>Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.</td>
<td>Modification of electronic records shall not obscure previously recorded information. The time source used by the system to timestamp the audit records must be secure from alteration by unauthorized users.</td>
<td>Modification of electronic records shall not obscure previously recorded information. The time source used by the system to timestamp the audit records must be secure from alteration by unauthorized users.</td>
</tr>
<tr>
<td>11.10(g)</td>
<td>Use of authority checks to ensure that only authorized individuals can: - use the system - electronically sign a record - access the operation or computer system input or output device - alter a record, or - perform the operation at hand.</td>
<td>The system must have identification and authorization controls to limit system access and all user actions within the system.</td>
<td>Testing of role-based security and access permissions to verify that user activities are restricted as appropriate to their role. Verify restrictions on: - System access (logon); - Use of electronic signatures; - Access to and use of system functions and operations; - Deletion and modification of records. (If deletion or modification of records (data) is permitted for certain individuals, then those alterations must be subject to audit trails.)</td>
</tr>
<tr>
<td>SECTION #</td>
<td>REQUIREMENT DEFINITION</td>
<td>INTERPRETATION</td>
<td>TESTING STRATEGY</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>11.10(h)</td>
<td>Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</td>
<td>The system must check the identity and validity of all data input devices/systems/instruments.</td>
<td>This is primarily relevant for systems that obtain data from other systems. Verify that inter-system communications are authenticated.</td>
</tr>
<tr>
<td>11.30 (Open System Only)</td>
<td>Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.</td>
<td>All electronic records that are transmitted over open networks (e.g. the Internet) must be encrypted while in transit. The encryption used must meet or exceed current good information security practices and standards.</td>
<td>For open systems, verify that transmitted electronic records are encrypted in transit. Document the encryption method(s) used and verify that they meet or exceed current accepted standards.</td>
</tr>
<tr>
<td>SECTION #</td>
<td>REQUIREMENT DEFINITION</td>
<td>INTERPRETATION</td>
<td>TESTING STRATEGY</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>11.100(a)</td>
<td>Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</td>
<td>The system must have controls to assure that each user has a unique user name and password combination, and to prevent user names from being reused</td>
<td>Verify that user accounts must have a unique ID, since two or more individuals can have the same password.</td>
</tr>
<tr>
<td>11.200(a)(2)</td>
<td>Electronic signatures that are not based upon biometrics shall be used only by their genuine owners.</td>
<td></td>
<td>Verify that an account cannot be deleted and then a new account with the same ID created.</td>
</tr>
<tr>
<td>SECTION #</td>
<td>REQUIREMENT DEFINITION</td>
<td>INTERPRETATION</td>
<td>TESTING STRATEGY</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>11.300(a)</td>
<td>Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.</td>
<td>The system must have controls to assure that each user has a unique user name and password combination, and to prevent user names from being reused.</td>
<td>The system must have controls to assure that each user has a unique user name and password combination, and to prevent user names from being reused.</td>
</tr>
<tr>
<td>11.30(b)</td>
<td>Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)</td>
<td>The system must have the capability to disable user accounts. The system must have the capability to force expiration of passwords after a configurable time period.</td>
<td>The system must have the capability to disable user accounts. The system must have the capability to force expiration of passwords after a configurable time period.</td>
</tr>
<tr>
<td>SECTION #</td>
<td>REQUIREMENT DEFINITION</td>
<td>INTERPRETATION</td>
<td>TESTING STRATEGY</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>11.300(c)</td>
<td>Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information and to issue temporary or permanent replacements using suitable, rigorous controls.</td>
<td>The system must allow an administrator to disable user accounts in the event that the account logon information is suspected of having been compromised.</td>
<td>Verify that an administrator can manually disable user accounts.</td>
</tr>
<tr>
<td>11.300(d)</td>
<td>Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.</td>
<td>The system must detect and log attempts at unauthorized use.</td>
<td>Verify that the system will log unsuccessful logon attempts and any use of the wrong password to perform electronic signatures.</td>
</tr>
</tbody>
</table>
CHAPTER 4: SECURITY CONSIDERATIONS FOR HOSTED DATA

- **Administrative Verifications:**
  - Data Security Policy, or equivalent *(Bonus Material)*
  - SOPs: Backup / Restore / Archive / Disaster Recovery
  - SOP (or equivalent) for Architecture Security & Maintenance: OS update, security patch implementation, software installation on hardware, etc…
Process Controls:

- Change Control Process.
  Note: externally hosted data is still subject to your Change Control

- Risk Management to determine where you’re at greatest risk for failure. Will drive the rigor of testing

- Employee Training: train employees to identify and report potential issues
Technical Controls:

- Verify Part 11 Requirements (Chapter 3)
- Controls for system access
- Controls of security access of your infrastructure hardware
Special Considerations for externally hosted Data (e.g. Cloud):

- Web-access system: Open or Close systems (per Part 11 definition)?

Ultimately, you decide: Is the 3rd party considered as an extension to your company (Close) or a different entity (Open)?

- Verify Data encryption: At rest and in transit (i.e. Open system part 11 requirement)

- Shared or dedicated application / web servers, for better security?
Auditing the hosting company: A Security Questionnaire might not be sufficient. Obtain the host QMS

How to ensure that you are aware of any change to infrastructure (e.g. OS, Patches, etc..) by the host?

In your Service Level Agreement (SLA)

How to verify that infrastructure changes by the host do not impact your data?

Remember: externally hosted data is still subject to your Change Control Process. Host cannot apply changes without your authorization!
CHAPTER 5: COMPUTER SYSTEM VALIDATION

5.1 V-MODEL

- User Requirements Specification
- Functional Requirements Specification
- Configuration and/or Design Specifications
- System Delivery / Implementation

- Verified in
- Verified in
- Verified in

- Performance Qualification
- Operational Qualification
- Installation Qualification
### 5.2 GAMP 5 CATEGORIES AND DELIVERABLES/EXECUTABLES

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
<th>Deliverables</th>
</tr>
</thead>
</table>
| **Category 1: Infrastructure software** | Software in this category provides the computing environment for running applications. Most common would be operating systems, programming languages, statistical packages, and network monitoring tools. | Combined statement of use and test plan | • Qualification testing  
• Report with TM |
| **Category 3: Non-configurable software** | Run-time parameters may be entered and stored, but the software cannot be configured to suit the business process. Or systems that are configurable but for which only the default configuration is used. | VP  
• Part 11 Assessment  
• URS  
• FRS  
• FRA  
• ADS | • IQ  
• OQ  
• PQ  
• TM  
• VSR |
<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 4: Configurable</td>
<td>Software that can be or must be configured by the user or the implementer to meet the specific needs of the user’s business process. Software code is not altered. <strong>Configuration</strong> is defined as the modification of the system-level functionality of a software product to meet business process or user requirements using tools provided by the supplier. This does not include modification of run-time parameters or user-specific functions.</td>
<td>• IQ • Config Verification • OQ • PQ • TM • VSR</td>
</tr>
<tr>
<td>Category</td>
<td>Definition</td>
<td>Deliverables</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| Category 5: Custom software | Software custom designed and coded to suit the business process. Customization is defined as the writing of novel software modules, scripts, procedures, or applications to meet business requirements. This can be achieved using an external programming language (such as C++ or Visual Basic for Applications or PL*SQL for database procedures), macro instructions, or an internal scripting language specific for a commercial application. | • VP  
• (Developer SQA audit for externally developed custom systems)  
• Part 11  
• URS  
• FRS  
• FRA  
• ADS  
• SDS  

• Software Design Review  
• Code Review  
• IQ  
• Unit Testing  
• Integration testing  
• PQ  
• VSR  
• TM |
## Other Types of Software (Non GAMP)

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
<th>Deliverables</th>
</tr>
</thead>
</table>
| “Helper” applications and software tools | Software applications that are not full computer systems by themselves, but are used to provide one or a few additional functions to computer systems. Individual integration tools out of a suite. | • Combined statement of use and test plan  
• Qualification testing to verify intended use  
• Report with TM |
| System Integrations | Subroutines, software modules or programs that are developed to connect functionality or transfer data between different computer systems. | • Combined Test Plan and Requirements  
• Design Specification  
• Design Verification  
• Qualification of any build tool(s) used  
• Verify functionality (e.g. data transformations)  
• Summary Report |
QUESTIONS