Manage data integrity in IT solutions

Scope

This instruction covers IT systems, IT infrastructure and computerised equipment (hereafter referred to as IT solutions) that handle GxP data in a supported/enabled GxP regulated process[1]. It describes how we use a risk-based approach to ensure the integrity of such data from the perspective of the individual IT solution.

As illustrated in *Figure 1*, the focal point of the instruction is a specific IT solution supporting (or enabling) part of a GxP regulated process and the related GxP data handled by the IT solution. As illustrated, the supported process and GxP data are typically part of overall flows involving more IT solutions (and possibly paper or similar).

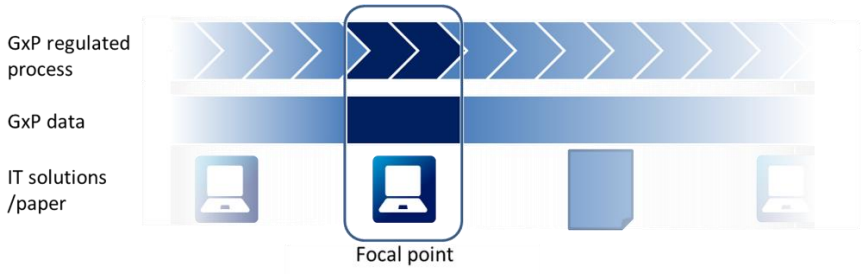


Figure 1: Focal point of the instruction and the wider context.

GxP data is data in electronic form required by relevant regulations, supporting GxP decisions, or necessary to reconstruct GxP activities *[Data integrity and data integrity governance at Novo Nordisk – Q0767307].* Understanding this scope is a prerequisite for determining relevant IT related data integrity risk controls (hereafter often just called 'controls'). Representatives of the process supported by the IT solution are responsible for identifying and specifying the GxP data in scope.

In accordance with risks, there is a particular focus on end users working with the GxP data. Ensuring relevant IT security controls according to *[Manage Information Security in IT Solutions – Q187655]*, including for privileged users, is a necessary prerequisite.

Note: Used terminology and roles are defined on the IT&Q Portal – this includes that

- *'IT solution' covers IT system/infrastructure and computerised equipment*
- *'IT Solution Manager' covers IT System/Infrastructure Manager and IT Responsible*
- *'IT Solution Owner' covers IT System/Infrastructure Owner and Computerised Equipment Owner.*

This also includes explanation of 'user', 'end user' and 'privileged user' (see 'privileged access rights').

[1] GxP regulated process: Any Novo Nordisk process that is subject to regulatory GxP requirements *[Novo Nordisk Quality Manual – Q166087]*

Not in scope
The instruction does not cover IT solutions where GxP data is

- only saved temporarily and cannot be modified or deleted, *and*
- output as a complete and accurate representation (for instance printed, transcribed from display or transferred to another IT solution).

This includes certain simple IT systems and computerised equipment used for direct printouts as stated in *[Good Documentation Practice and Data Integrity - Q054929].*

Note: Such IT solutions are still part of the overall data flow setup (as illustrated in Figure 1), the data is still GxP data, and the IT solution itself is still GxP critical, but it is not subject to specific data integrity considerations due to this instruction. However, the IT solutions must still comply with the requirements for the GxP data according to for instance [Good Documentation Practice and Data Integrity - Q054929].

Applies to

The instruction applies to

- roles with responsibilities for managing IT solutions, for instance:
    - IT Project Manager responsible for an IT project
    - IT Responsible or IT Solution Manager responsible for the day-to-day operation of an IT solution
    - Roles with delegated responsibilities, for instance a consultant who performs IT tasks or an IT SME (Subject Matter Expert), including Professional/Citizen Developers
    - Risk Managers with responsibilities in relation to the IT risk assessment.
- QAs with responsibilities for IT solutions in scope of this instruction.

Note: The instruction does not apply to end users of IT solutions.

Reader's guide

Appendix A and B are followed by completing the mandatory IT risk assessment in ServiceNow IRM. You must still follow the remaining part of the instruction including the process as described.

Table of contents

1. Introduction

Where our IT solutions handle GxP data, we safeguard the integrity of these data by ensuring that an adequate set of data integrity controls is built into the IT solutions.

As illustrated in *Figure 2*, GxP data flowing in a GxP regulated process (see *Figure 1*) follows a lifecycle, in which data is created, used and retained/archived according to requirements to the process, and if relevant destroyed:

Figure 2: Data lifecycle phases

During this lifecycle, data integrity is challenged by various risks that can be mitigated by data integrity controls with contributions from business and IT.

Figure 3 provides a model for the data lifecycle seen from the perspective of the IT solution covering part of process and data flows illustrated in *Figure 1*. The model is the outset for the risk-based approach applied in this instruction.

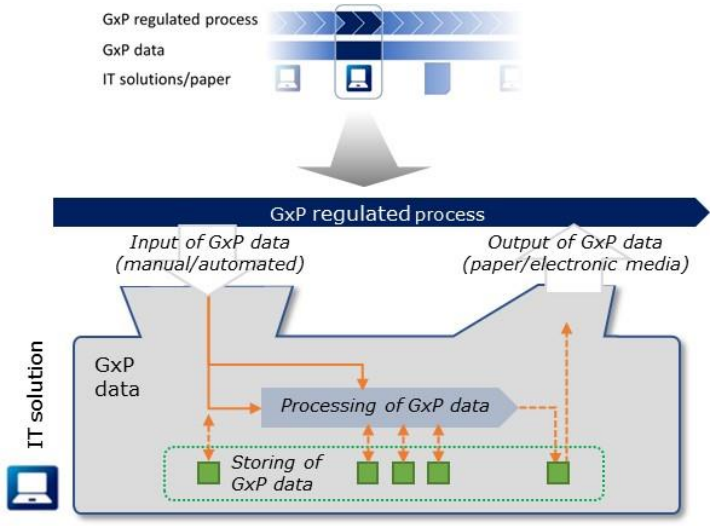


Figure 3: Conceptual model of an IT solution (where IT infrastructure is considered part of the IT solution) and GxP data. 'GxP data input' in the GxP regulated process enters the IT solution, is processed and stored and eventually leaves the IT solution as output. 'GxP data input' can be manually entered, captured electronically by input devices (such as bar code scanners and measuring equipment), or transferred from another IT solution. Processing of GxP data can involve end users or be automated/digitalised. 'GxP data output' can be written by the IT solution to for instance paper, electronic media (such as displays, file shares or external hard discs) or transferred to another IT solution.

2. Assess IT data integrity risks and determine IT related data integrity controls

An IT risk assessment with focus on data integrity risks must be performed by relevant stakeholders to assess which risks are relevant for the IT solution and the integrity of the GxP data in scope.

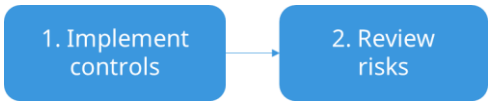
This data integrity risk assessment and the determination of controls are integrated in the mandatory IT risk management process in ServiceNow IRM and therefore not necessarily performed in isolation, but as part of assessing a broader set of risks related to the IT solution.

Detailed steps are as follows:

Responsible: IT Solution Manager or delegate		
Action		**Description**
1	Identify stakeholders	Identify all processes supported by the IT solution and its GxP data in order to identify the right group of stakeholders. Relevant stakeholders covering knowledge about the IT solution, GxP data and processes include • Risk Manager • Data Owner(s) or Data Responsible Person responsible for the GxP data handled by the IT solution [*Good Documentation Practice and Data Integrity - Q054929]* • Line of Business SMEs who understand the processes and GxP data, as relevant • IT solution SMEs who have insight into the technical setup of the IT solution, as relevant • QA who understands which quality requirements apply to the process and GxP data.
2	Assess risks	Answer all questions in appendix A and B by completing the relevant part of the IT risk assessment in ServiceNow IRM. This is done in collaboration with the identified stakeholders. *Note: As the assessment of risks and identification of relevant controls depends on an understanding of the IT solution in context of the supported process and GxP data flow, it is highly advisable to have descriptions of scope of GxP data as well as process flow and data flow available.*
3	Determine controls	ServiceNow IRM will output the data integrity controls that are relevant to address.

Responsible: IT Solution Manager or delegate		
Action		**Description**
		For each control: Determine and document how to apply the control. Consider the relevance of controls in the complete process flow and data flow supported by the IT solution. *Example: End users in a process must be able to change GxP data at three points of the data flow – this will require an audit trail. When describing how to apply an audit trail, all three instances should be identified rather than just stating that audit trail must be available.*

3. Implement and maintain IT related data integrity controls



The IT data integrity controls identified in section 2 must be implemented and maintained. If a determined IT data integrity control cannot be implemented, for instance for technical reasons, this must be raised to the IT Solution Owner who decides how to proceed.

The adequacy of implemented data integrity controls is evaluated and followed-up on at a regular basis.

When retiring an IT solution handling GxP data, follow the approach in appendix C.

Responsible: IT Project/Solution Manager or delegate		
Action		**Description**

1	Implement controls	Ensure that the determined IT data integrity controls are specified in relevant documentation for the IT solution according to the completed IT risk assessment.
		
		Depending on the individual control, this may be:
		• Technical controls in specification, such as
		  ○ functional / technical design specification
		  ○ IT infrastructure requirements specification.
		• Procedural controls, such as
		  ○ operation and maintenance document
		  ○ Service Level Agreement (SLA)/contract with supplier
		  ○ internal interface agreement.
		
		Ensure traceability between identified risks and implemented controls.

2	Review risks	Review the completed IT risk assessment in ServiceNow IRM with focus on data integrity risks and controls considering emerging

Responsible: IT Project/Solution Manager or delegate		
Action		**Description**

		knowledge and experience to ensure that the implemented controls remain effective and relevant. This must be done at least every three years or when
		• a change to the IT solution (including technology) may
		  ○ impact the adequacy of implemented controls or
		  ○ provide new opportunities for more effective controls
		• a change in the way the GxP data is used in the process may change the need for controls in the IT solution.
		
		Update the IT risk assessment in ServiceNow IRM to reflect any changes. Implement new and remove obsolete data integrity controls accordingly.
		Note: Evidence of the review is ensured by the use of ServiceNow IRM.

Appendix A: List of IT related data integrity risks and related controls

The below risks are assessed, and controls identified as relevant. This is done by using the IT risk assessment in ServiceNow IRM.

ID	Risk area	Specific risk consideration	IT data integrity control
1-1	Input of GxP data	Incorrect input GxP data not being identified by the process.	Input GxP data must as relevant and possible be verified by the receiving IT solution. *Note: This also applies to automated transfer processes (e.g. transferring GxP data from another IT solution) .* *Note: 'Verified' in this context means ensuring compliance with specifications as defined by the supported process.* *The extent of verification to be performed for the IT solution depends on the specific circumstances including what verification will take place in the process.*
1-2	Input of GxP data	N/A	Input GxP data must include the originator of the data (the specific end user or IT solution). *Note: This also applies when GxP data is delivered from an external supplier.*
1-3	Input of GxP data	Mix up of GxP data in connection with use of input devices	The validity and connection of input devices (such as bar code scanners or specific measuring equipment) must be checked. *Note: This check may be built into the IT solution as an automated check, or it may be part of the installation verification.*
1-4	Input of GxP data	N/A	GxP data must be automatically saved sufficiently frequent for the GxP data time stamp and the time of data entry to be correctly aligned.
1-5	Input of GxP data	N/A	GxP data must be automatically saved sufficiently frequent to ensure that potentially unacceptable changes may be detected. Saving must be performed per field (unit of data), unless a documented assessment considering risks in the supported process concludes that the above may be achieved by other means (e.g. by saving per group of fields). *Note: Automated saving is performed for instance per field, group of fields or screen. Such saving will ensure that subsequent changes are captured in an audit trail according to ID 3-2, thereby available for users' review.*
2-1	Processing of GxP data	Critical workflow steps not executed in the correct sequence.	The IT system/CE must be equipped with functionality that mirrors the required sequence of steps. *Note: A required sequence of events could for instance be a workflow setup to ensure that entry of GxP data is completed before review, and that review is completed before approval.* *This also implies that to fulfil ID 1-4, GxP data entries must be saved contemporaneously per step for the time stamp to reflect the correct sequence.*

ID	Risk area	Specific risk consideration	IT data integrity control
3-1	Storing of GxP data	N/A	a. Stored GxP data must include time stamp ('GxP data time stamp') reflecting when GxP data were created. b. Date and time used in GxP data time stamps must be synchronised based on a reliable system clock. c. GxP data time stamp must be recorded and displayed in the 'official time' of the location where the data were created. If this is not possible, 'NN time' can be used instead. *Note: Users entering or reading such time stamps must be provided with a clear understanding of the time zone used.* *Note: For further details, including definition of 'official time' and 'NN time', see [Good Documentation Practice and Data Integrity - Q054929].*

3-2	Storing of GxP data	User able to create, modify or delete GxP data via the user interface.	a. IT system/CE generated audit trails must be established. The audit trail must document
			• *who* performed the entry or action (user ID, for example the NN employee initials),
			• *when* it took place ('GxP data time stamp'),
			• *what* was created/modified/deleted (including as relevant the type of end user entry or action),
			• *why* (reason for change), where
			  ○ required by GxP regulations, or
			  ○ important to the process, but not obvious from the context.
			b. Audit trails must be available for users' review of changes to GxP data as part of the process, retained for a period at least as long as that required for the GxP data, and available for inspection together with the related GxP data.
			Note: This means that the audit trail must be presented to end users in a human readable form in the complete retention period.
			Note: Audit trail may be implemented as a list of changes or by saving all versions (from which audit trail can be generated). For documents this is implemented by change log (capturing what and why), and document information (capturing who and when).

3-3	Storing of GxP data	N/A	If a user can change audit trail functionality (including deactivation and reactivation) via the user interface, this must be automatically captured in a system audit trail and regularly reviewed. If possible, this capture must be combined with the audit trail in ID 3-2. If not, it must take place in another automated solution with similar data integrity controls. *Note: Authorisation to deactivate audit trail functionality via the user interface should only be provided to privileged users as needed, and it should never be provided to end users able to create, modify or delete GxP data via the user interface (follows from ID 5-1)*

ID	Risk area	Specific risk consideration	IT data integrity control
3-4	Storing of GxP data[2]	N/A	a. GxP data must be stored and preserved throughout the data lifecycle in a form fit for the intended use of the GxP data. This includes, that the dynamic character of the GxP data must be preserved in a form fit for the intended use, for example to allow zoom in on, search, sort and trend of the data. b. GxP data must not be deleted in the retention period, unless previous content and meaning can be reconstructed based on audit trail, or GxP data have been transferred according to ID 4-4. *Note: This means, that changes to data format, that impacts the readability, such as encryption, coding or compression, must be completely reversible.* c. GxP data must not be temporarily saved in a manner allowing for manipulation or loss, before being stored safely and securely. This also means that the media used for storage of GxP data must be durable. d. Backup copies of GxP data must have the same appropriate level of controls as the GxP data itself to prohibit unauthorised access to, changes to and deletion of the data. *Note: Based on decision by Data Owner or Data Responsible Person, GxP data can either be retained in the IT solution where it was created and used or be moved to a dedicated electronic archiving solution (following ID 4-4).*
4-1	Output of GxP data[2]	Automated transfer processes corrupting integrity of GxP data.	Automated transfer processes (for example transferring GxP data from one IT solution to another) must include a built-in verification mechanism that ensures that the GxP data is correctly transferred.
4-2	Output of GxP data[2]	End user able to control what GxP data is selected for output for GxP use, and/or how the output is presented.	a. Any end user selection of GxP data output must be presented together with the output. b. Any end user selection of how the output is presented must be presented together with the output.

[2] Note that in this context GxP data (besides associated metadata such as audit trail) also includes applied GxP signatures.

ID	Risk area	Specific risk consideration	IT data integrity control
4-3	Output of GxP data[2]	N/A	It must be possible to generate accurate and complete copies of GxP data, including audit trails and any GxP signatures, in a form maintaining content and meaning, including any relevant ability to zoom in on, search, sort and trend data. *Note: This includes copies made available for inspection review and copying. Maintaining contents and meaning implies that a dynamic data file format must be used.*
4-4	Output of GxP data[2]	N/A	a. Content and meaning (including readability) must be preserved when GxP data is transferred from the IT solution, that is: • migrated to another IT solution/electronic storage, or • converted to a readable electronic format (such as PDF or XML) or printed to paper. b. Any transfer of GxP data must take outset in a risk-based decision by Data Owner or Data Responsible Person which is: • justified to GxP regulations, including preservation of the dynamic character of the GxP data (according to ID 3.4a), • determined in advance and documented. c. It must be verified, that the transfer process maintains content and meaning of the GxP data, either by verification of the transferred GxP data or by a validated automated transfer. *Note: Preserving content and meaning implies that all GxP data, including meta data and GxP signatures are transferred.*

5-1	Access by user	N/A	a. User profiles (roles) must be defined according to required privileges /authorisations.
			b. User profile privileges must be limited to those required for individuals to perform their role/ duties ('least privilege' principle).
			c. Assigning user profiles to users must comply with the principle of 'separation of duties'.
			Note: This implies for instance that
			• *privileged users do not perform end user tasks in the IT solution and are independent from end users performing such tasks.*
			• *privileged user profiles are not assigned to individuals with a direct interest in GxP data (for instance data generation, data review, data approval or applying GxP signature).*
			• *end users must not be able to modify*
			  ○ *entries in the audit trail*
			  ○ *audit trail functionality*
			  ○ *source of date, time and time zone, when this is captured by the IT solution and used as a GxP data timestamp*

ID	Risk area	Specific risk consideration	IT data integrity control
5-2	Access by user	User able to create, modify or delete GxP data, or apply GxP signature, via the user interface.	User profile must be assigned to (and thus traceable to) an individual user. *Note: This implies that under such circumstances, user profiles designed for login by more than one user ('group accounts') are not allowed. And the user profile may only be used by the assigned user.*
5-3	Access by user	Privileged users able to create, modify or delete GxP data outside the user interface.	a. If GxP data changes are performed, these must be duly authorised by Data Owner or Data Responsible Person. b. User profile must be assigned to (and thus traceable to) individual user, where this is supported by the IT setup.
6-1	N/A	Unacceptable additional risks to data integrity are identified.	Identify and implement additional mitigating controls as needed. *Note: Apply critical thinking to identify any additional risks that may apply in addition to the generic risks (ID 1-1 to 5-3 and 6-2.*
6-2	N/A	Unacceptable risks to data integrity associated with identified failure modes in the IT solution.	Assess and address identified failure modes and implement mitigating controls. It may be relevant to regularly review system audit trails (e.g. system or event logs) as risk mitigation. *Note: Failure modes are technical errors or other technical limitations in the IT system impacting the functionality.* *Failure modes may for instance be identified during the design phase, from supplier information, via information from Line of Business or as part of deviations. Such failure modes do not include issues in the supported processes, for instance those covered by [Manage Alarms and Warnings - Q102982].*

Appendix B: Requirements for implementation of GxP signatures

ID	IT data integrity control (requirement)
7-1	A GxP signature must • uniquely identify the signer (such as NN initials) • authenticate the signer To authenticate the signer, the signer must at time of signing use at least one of the following methods: • Password • Biometric (such as face or fingerprint) These authentication methods may be combined with additional security (such as an authentication app on a phone or a cryptographic key). The solution must ensure non-repudiation, meaning that the signer cannot later deny having signed the record. It must not be possible to misuse an unattended or unlocked device for signing. *Note: Complexity of password depends on how this is combined with other methods adding additional security, and this may for instance mean that a PIN or another memorised credential is acceptable.*
7-2	When a user signs GxP data electronically using a GxP signature, it must be clear to the user what GxP data is signed an what the meaning is (for instance: 'Reviewed', 'Approved', 'Rejected').
7-3	N/A (requirement has been included in 7-1)
7-4	The GxP signature must be permanently linked to the GxP data being signed, and it must not be possible to modify or remove a GxP signature and/or re-apply it elsewhere by ordinary means (for instance using of standard system functionality or commonly available desktop tools). *Note: It follows, that if a signed record is changed, it must appear unsigned (i.e. the existing signature is removed or clearly marked as invalid).*
7-5	When a user with no permission tries to sign, this must be rejected and logged by the IT system/CE.

ID	IT data integrity control (requirement)
7-6	When a GxP signature is applied on GxP data, the IT system/CE must automatically record: • An indication that the GxP data have been electronically signed • The 'printed' (full) name or the NN-initials of the signer • The date and time of the signature (traceable to the local time relative to the signer) • The meaning of the signature. *Note: NN initials may be included as an alternative or supplement to the full name.* *NN employees are uniquely identified by NN initials. The translation from NN initials to the person's name can be performed at any time, since:* • *NN initials are never changed or reused,* • *a link to the person's full name is retained, and* • *the name is kept up to date (if changed) while employed at NN.*
7-7	When signed GxP data (according to ID 7-1 – 7-6 and 7-8) are displayed - either on a screen or as hard copy – the signature manifestation of the GxP signature (ID 7-6) must be included. *Note: It is acceptable to show name or NN initials. See also note in 7-6.*
7-8	N/A (requirement has been removed)
7-9	If a hybrid solution is chosen, where the GxP data is stored electronically but the GxP signature is on paper: The signed paper must clearly link to the covered GxP data by showing the necessary information (e.g. the identity of the IT system/CE used and the date of print generation). *Note: As GxP data must be stored and preserved throughout the data lifecycle, the signature including the link must be unbreakable.*
7-10	As additional IT security controls, procedures must be in place for: • Initial and periodic testing of devices, such as tokens or cards with user ID/password information in order to ensure that they function properly and have not been altered in an unauthorised manner. • Managing situations where users have forgotten the password or lost their tokens or some other means of electronic identification. These procedures include the de-activation of the lost password and the issuing of a replacement password, either temporarily or permanently. • Detection, reporting and actions to be taken in a timely manner in case of attempts of unauthorised access to the IT system/CE and unauthorised attempts to sign with GxP signature.

Appendix C: Retirement of IT solution containing GxP data

This appendix describes the approach to take when an IT solution containing GxP data is planned not to be used any more (either to be retired or will no longer be supported).

Depending on where GxP data is in the lifecycle, it must either be retained (use or retain/archive phase) or may be deleted (destroy phase).

When GxP data is to be retained:

GxP data must be transferred from the IT solution according to Appendix A, ID 4-4.

When deciding on the approach for GxP data in the retain/archive phase, consider practicality and long-term suitability of the IT solution (for instance if considering maintaining existing software in a virtual environment)

When migrating GxP data to another IT solution or storage medium:

- Migration must be based on a defined process, including a documented risk assessment, and managed within the framework of data migration planning and reporting.
- Verification of migrated GxP data must be documented.

Where GxP data is migrated from one IT solution to another, IT Solution Owners (or delegates) from both IT solutions must be involved.

When GxP data is to be deleted:

GxP data may only be deleted when decided according to [*Protecting and Handling Information – Q190751*] and following a procedure defined by the Data Owner or Data Responsible Person and including management authorisation.

Document Approvals

Approved Date: 13 Dec 2024

Task: Approval Verdict: Approve changes & release	KAL (Kristian Alkjærsig), (kal@novonordisk.com) Content Responsible 12-Dec-2024 07:03:24 GMT+0000

Task: Approval Verdict: Approve changes & release	PLB (Peter Lorentz Bagger), (PLB@novonordisk.com) Content Owner 12-Dec-2024 13:33:08 GMT+0000

Task: Approval Verdict: Approve changes & release	TMJI (Mohit Jain), (TMJI@novonordisk.com) QA 13-Dec-2024 08:01:03 GMT+0000