Medicines & Healthcare products Regulatory Agency

MHRA Regulating Medicines and Medical Devices

Comment sheet for MHRA draft document:

MHRA GxP Data Integrity Definitions and Guidance for Industry

Deadline for comments: 31 October 2016

Send comments in Word format to: inspectorate@mhra.gsi.gov.uk

Comments from:

Name of organisation or individual
ISPE – International Society for Pharmaceutical Engineering 7200 Wisconsin Ave., Suite 305 Bethesda, MD 20814 USA Tel. +1 301-364-9201 www.ispe.org

Please be aware that information submitted may be made public under a Freedom of Information Act request. Please highlight any information considered commercially sensitive.

1. General comments:

Please include rationale / background to any general comments.

1. ISPE members welcome this guidance as an important step to the continuing effort by regulatory authorities and industry to guarantee data integrity and we greatly appreciate the opportunity to review and comment on it. MHRA's expansion of their guidance to encompass GxP systems is a very positive and welcomed trend since it clearly emphasizes the importance of data integrity throughout the product lifecycle. We also support the linkage to criticality and inherent integrity risk that the MHRA continues to emphasize throughout its guidance. Understanding our business processes and the potential data risks are paramount to ensuring the integrity of the data and products we generate and ultimately patient safety.
2. Additional consideration is recommended for "simple systems" that are based on very standard desktop type tools (Excel, Sharepoint) where the records may have an indirect GxP impact. Achieving "full" compliance with this guidance may appear to preclude the use of such tools.
3. Using consistent criteria for determining the criticality of data is recommended; line 32 – "... impact to the patient and environment", line 57 – "...impact to quality attributes", lines

96-97 – "...impact to product and patient", lines 383-384 – "…to ensure safety of the subject or quality of the product or data."

4. Replacing data "checking and cross-checks" (e.g. line 35, 65), with "reviewing or reviews", is recommended
5. Please clarify that the guidance applies only to GxP **data.** Many information **systems** (computerized or paper) hold and process GxP and non-GxP data and it is therefore important to differentiate between the two.
6. Please define the terms "static data" and "dynamic data".
7. The date for using compliant systems with individual accounts and audit trails is the end of 2017 (same as the date of the GMP Guidance) even though the scope of this guidance is broader than the GMP one, released more than a year earlier. We are concerned that this may be an insufficient time interval for compliance of GxP (but not GMP) systems. Extending the time to comply with the guidance beyond 2017 for all GxP data using individual accounts and audit trails, would allow industry sufficient time for a more thorough approach.
8. Regarding Dynamic Data: Some record retention requirements for clinical trial (CT) related data are over 30 years old. Retaining the dynamic nature of the data is likely not feasible for this time period because of technical constraints and availability of useable hardware. Furthermore, with time, the dynamic nature of some data will decrease, and having a more flexible approach to ensure the availability of the data and metadata should be appropriate. We recommend considering a more flexible, risk based preservation of "dynamic data."
9. Complying with the requirements for no shared user accounts and no shared accounts for system administration by the end of 2017 is a time frame of concern to industry. This concern was also raised with the previous MHRA guidance. In addition, clarification is requested as to how this requirement applies to all regulated computerized systems, including back end databases and low level functionality, since some of these systems have shared administrator accounts by design. There are also embedded control modules on equipment that allow access at the IP address level or a specific tag name level – these systems are very low risk and do not appear to meet the intent of no shared accounts
10. Please clarify that error checks for manual data entry are acceptable and important practice. As written, Section 12 Computer system transactions of the guidance, could be interpreted as prohibiting the common and standard practices of error detection during manual entry. This practice generally improves the overall integrity and quality of the manually entered data. With respect to the design of computer systems, please clarify that the immediate commitment of critical data to permanent memory is not intended to be an audit trail of every keystroke.

2. Specific comments on text:

Line number(s) of the relevant text *(e.g. Lines 20-23)*	Comment and rationale	Proposed Change (if any) *(If changes to the wording are suggested, please highlight using 'track changes')*
32-33	Clarification is requested regarding the use of the term “environment”. Is the intent “harm to the environment”? This may be beyond the scope of this guidance. We recommend removing the use of this term.	The effort and resource applied to assure the validity and integrity of the data should be commensurate with the risk and impact of a data integrity failure to the patient safety or quality of the product ~~environment~~.
37-41	If there is an expectation that the supporting rationale would be documented for the state of control on data integrity risks, we suggest adding language to clarify what is expected within the documented rationale Need to clarify the specific expectations related to periodic system review; does that mean computer system or "system" in the broader sense? In either case, the “effectiveness of existing control measures” and to “consider the possibility of unauthorised activity” are both ambiguous and subject to misinterpretation. If the intent is to address computer system related reviews, we suggest including access roster reviews and monitoring for unauthorized access attempts.	For example, could add the following: “…control based on the data integrity risk with documented supporting rationale.” In addition to routine data review, the wider data governance system should ensure that periodic audits are capable of detecting opportunities for data integrity failures within the company’s system, e.g. routine data review should consider the integrity of an individual data set, whereas the periodic system review might verify the effectiveness of existing control measures and consider the possibility of unauthorised activity.

59 Similar change to 316	To allow for the guidance to apply to both manual and electronically generated data, suggest eliminating the word "manual" and add "an activity" The use of Hybrid systems should also be addressed.	"…Data may be generated ~~by~~ (i) ~~manual means~~ on paper – a paper-based record of an ~~manual~~ observation or of an activity or (ii) ~~electronic means~~ electronically - in terms of equipment, a spectrum of simple machines through to complex highly configurable computerised systems. Add (iii) or using a hybrid system of both paper-based and electronic records"
81	Large and complex systems like Enterprise resource planning (ERP), could generate a printout that is representative of the original data, and may fully preserve GxP content and meaning. The guidance should consider the use of these large complex systems.	Please Change text: "Printouts not representative of original data" to "Printouts less likely to be representative of original data" Please also change text: "Printouts may represent original data" to "Printouts likely to represent original data".
97-98	The sentence is written with a double negative which makes interpretation difficult. We recommend clarifying the sentence in a positive voice.	Reduced effort and/or frequency of control measures may be justified for data that has a lesser impact to product and patient, or if those data obtained from a process can only be amended through specialized knowledge or software"
124	Recommend clarifying the sentence or removing the phrase, "or audit trail." The system design should prevent users from accessing unauthorized data amendments. Having audit trails to monitor such activities is a separate design requirement.	Does this mean to either prevent this action **or** an audit trail
153	The definition of Data (*facts and statistics collected together for reference or analysis*) leaves it open to wide interpretation. Specifically, many Computerized Systems hold Data that has potential to impact Pharmaceutical Quality and Consumer Safety and Data that has no potential to impact	The definition of data needs be adjusted to the following text to avoid misinterpretation: "*Facts and statistics*

	Pharmaceutical Quality and Consumer Safety.	*that are collected together for reference or analysis, and have the potential to impact product quality or consumer safety."*
160 and 169, also 343-345, 532-533	Please clarify when it is permissible to replace an original record with a true copy. In recent MHRA GCP forum (25Nov2015) pertaining to retention of trial records, the MHRA provided the advice to retain all original trial essential documents (including trial medical records) for at least 5 years after completion of the trial. If, after that time, the documents are required by regulatory authorities (e.g. in support of applications for marketing authorisation) and original paper records were destroyed in favour of electronic copies, the electronic data would only be acceptable if they meet conditions in the previous paragraph".	Delete true copy as an acceptable form of data in all cases. What is the true expectation?
163-164	Recommend using the term ALCOA+, where the + is complete, consistent, and enduring. Use (data) lifecycle for consistency (see 217)	Data governance measures should also ensure that data is ~~compete~~ complete, consistent and enduring throughout the data lifecycle
173-174	Expand the definition to explain that raw data is data that has not undergone <u>any form</u> of processing.	The definition of 'original records' currently varies across regulatory documents. By its nature, paper copies of raw data generated electronically cannot be considered as 'raw data'. Raw data is data that has not undergone any processing, either manually or through automated computer software.
247	Please clarify the expectation for the phrase 'directly accessible on request from national competent authorities.' Is this indicating that inspected sites should provide direct system access to inspectors and if so to what level?	
254	Recommend adding the word, "transfer" as a step in the data lifecycle. Transfer is defined as the movement of data from one system to another interface.	"..processing (including transfer, analysis, transformation or migration).."

266-267	Recommend emphasizing the 'objective' of data transfer / migration.	……Data migration changes the format of data to make it usable or visible on an alternate computerised system. The ultimate goal of any data migration is to have data that remains both usable and retains its contextual meaning.
337-338	*The copy may be verified by dated signature or by a validated electronic signature.* This statement does not allow for verification of true copies by means of automated processes that have been validated.	*Suggested edit: The copy may be manually verified by dated signature or by a validated electronic signature, or by an automated and validated process.*
338-340	*A true copy may be retained in a different electronic file format to the original record, if required, but must retain the equivalent static/dynamic nature of the original record.* This statement '...must retain the equivalent...' contradicts statements in 351-352 and 359-367 both on which state that consideration should be given to the form of retained electronic records. In many cases it is highly beneficial to the integrity of an electronic record that is no longer active to archive it into a static format (such as pdf). This minimizes the risk of obsolescence of the means by which the record is interrogated (the software required to read it), and minimizes the risk of wilful or unintentional change of its content. It is also perfectly possible to archive to a static format while retaining the full data meaning (meta data) and audit trail.	*A true copy may be retained in a different electronic file format to the original record, if required, but must retain the meta data and audit trail required to ensure that the full meaning of the data is retained and its history may be reconstructed.*
354-357	The original language introduces the term certified copies, within the section on true copies. If the intent is that a certified copy is the same as a true copy, recommend using the same language to avoid confusion As a follow up to the above question, please clarify what constitutes 'authority' in this statement?	"Where true copies of documents are made, the process to confirm the true copy contains the same attributes and information as the original should be described…….and for identifying the party who made the true copy." ".. and for identifying the certifying party and their authority for making that copy."
359-367	Dynamic data retention and conceivability for conversion to static data. Dynamic data can become/ be retained as static data, but the requirements to do so are significant	Include clarification of what is meant by all data and the use of risk-based

	based on this section. Applying these expectations, especially "verified copies of all raw data, metadata, relevant audit trail and result files" to data later in its data lifecycle may not be feasible or appropriate. Does this mean that verified copies of ALL data must be retained, or can a risk-based approach with an appropriate rationale on a representative sample of the data be used to justify confidence in the integrity of the data? Furthermore, are there cases later in the lifecycle where just a documented rationale would be appropriate due to the criticality and use of the data? Consideration should be given to the 'age' of the dynamic data and its criticality throughout its retention period as to whether complete reconstruction is necessary.	documented rationales and approaches for verification to justify the integrity of dynamic data when converting it to static data, especially late in a data lifecycle as the data gets "older" and the need for complete reconstruction is not as critical.
372-389	Section 12 Computer system transactions: The first two paragraphs (lines 372-375 and 377-379) seem to contradict the last paragraph; If you must have a deliberate act to create an ER then this seems contradictory to the last paragraph (386-389) of this section. It is unclear if the intent was to not save until a user hits a save button (i.e.; FTIR or HPLC). Common practice is for audit trails to not capture every key stroke and mistake that is held in a temporary buffer before those commitments. For example, where an operator records the lot number of an ingredient by typing the lot number, followed by the ''return key'' (where pressing the return key would cause the information to be saved to a file), the audit trail need not record every ''backspace delete'' key the operator may have previously pressed to correct a typing error prior to committing the value. Subsequent ''saved'' corrections made after such a commitment, however, must be part of the audit trail. If data can be saved after a deliberate act or forced by the system, users will most likely default to a deliberate act (much easier to comply with).	Please ensure consistency of the language and clear expectations across this section. Please define the circumstances under which data should be saved under a deliberate act or when forced by the system.
443	*Section 14. currently states:* *"The use of electronic signatures should be compliant with the requirements of international standards such as Directive 1999/93/EC (requirements relevant to 'advanced electronic signature')."* The implication or expectation that the use of electronic signatures for GxP purposes should comply with Directive 1999/93/EC relevant to 'advanced electronic signature implies the need for technical requirements beyond those applied to the majority of electronic signatures currently used for GxP purposes within regulated companies." The term 'advanced electronic signature' implies the use of third party certification and cryptographic techniques specifically intended to ensure that any subsequent change of the data is	Remove the statement: *"The use of electronic signatures should be compliant with the requirements of international standards such as Directive 1999/93/EC (requirements relevant to 'advanced electronic signature')."*

	detectable. To be compliant with the Directive requirements relevant to advanced electronic signature implies that all compliant electronic signatures must be "Digital Signatures" as defined by US FDA CFR Part 11. *"Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified."* We believe that the Directive is not directly applicable to electronic signatures applied for GxP purposes within the boundaries of the regulated company. The Directive is intended to establish a legal framework for electronic signatures and certain certification-services "in order to ensure the proper functioning of the internal market", i.e. specifically for inter-party commercial and financial transactions. Additionally the Directive itself notes that a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified numbers of participants. The vast majority of electronic signatures applied to electronic records in the GxP environment are "electronic signatures" (as per EU GAMP and FDA terminology) and are not "digital signatures" (FDA) or "advanced electronic signatures" (EU Directive), and these are (absent other deficiencies) compliant with current GxP regulations (EU and US). Compare also the following text from Annex 11 (underline added): *14. Electronic Signature* *Electronic records may be signed electronically. Electronic signatures are expected to:* *a. have the same impact as hand-written signatures <u>within the boundaries of the company</u>,* *b. be permanently linked to their respective record,* *c. include the time and date that they were applied.*	

	As we noted in the ISPE published GAMP interpretation of Annex 11: *The phrase "within the boundaries of the company" clarifies that such signatures applied to records maintained by the regulated company are not subject to Directive 1999/93/EC on a Community framework for electronic signatures, nor the 2000/31/EC Directive on electronic commerce, nor any associated national regulations of EU member states on such topics.* *The approach is consistent to that described in in the US FDA Part 11 Scope and Application Guidance* In conclusion, the implication or expectation that the use of electronic signatures for GxP purposes should be compliant with the requirements of Directive 1999/93/EC relevant to 'advanced electronic signature' is excessive if taken literally, and would at the very at least cause industry confusion and misunderstanding on the distinction between electronic signatures and digital signatures, and on the acceptability of normal and typical GxP electronic signatures.	
456 and 458	The first sentence of the paragraph mentions both data review and approval. However, the section header and section content does not specify approval or provide any expectations regarding data approval.	Recommend deleting approval or if retained, modifying the header and content to reflect the expectations for data approval.
487-499	Shared logins/ generic user accounts – Is there a similar expectation for clinical systems regarding replacement by the end of 2017? The directive only applies to GMP systems.	Clarify the applicability of this to GxP systems, or if it only applies to GMP systems.
503	Where unique login credentials are not possible for system administrator accounts or other accounts with some type of privileged access, other mitigating controls that reduce the risk to an acceptable level should be allowed. Regulations such as 21 CFR Part 11 focus on the need for audit trails when electronic records are being created, modified, or deleted or when actions required by regulation are being tracked (e.g., acknowledging critical alarms). Accounts used for these purposes must log in with unique credentials to meet this requirement. However, other accounts that may have an indirect impact (e.g., accounts used to modify system parameters or configuration) on electronic records where processes such as change control are required to make such modifications have a lower risk profile and suggest that a risk-based approach be allowed when these types of accounts are shared.	Personnel with system administrator access should log in with unique credentials that allow actions in the audit trail(s) to be attributed to a specific individual. If this is not possible, mitigating controls that reduce the risk to a level deemed acceptable based on the impact to product quality and patient safety are allowed if this rational is approved by appropriate members of the Quality Unit.

	This also aligns with EU GMP Annex 11 that allows for a risk based approach for audit trails. Excerpt from Annex 11: 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.	
522	Neither Data retention nor Archive sections provide any guidelines in data retention time periods, or indicate where that information can be found. Is this intended?	Clarify that data retention time periods are as specified in the respective GxP predicate regulations somewhere in the section starting line 522.
549-554	This paragraph is focused extensively on “how to” maintain legacy system data and little on the purpose for doing so. The basic requirement is that data (entire record) must be retained throughout the retention period and the format and ability to continue to process data should be determined based on risk and value of the data over time. Retaining legacy software or using outsourced solutions such as the cloud are business decisions on how to achieve the requirements. Use of the example “SaaS” as a possible solution is not always applicable as very few of the systems used in GxP world are even available as Software as a Service (SaaS) solutions. Consider stating it as “a data archival process must preserve the integrity of the data such that the qualities of that data are preserved and GMP decisions based on that data are not compromised.”	The archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period. In the case of electronic data archival, this process should be validated, and in the case of legacy systems the ability to review data periodically verified (i.e. to confirm the continued support of legacy computerised systems). ~~When legacy systems can no longer be supported, consideration should be given to maintaining the software for data accessibility purposes as long as reasonably practicable. This may be achieved by maintaining software in a virtual environment (e.g. Cloud or SaaS).~~ Migration to an alternative file format which retains the ~~‘true copy’ attributes of the data~~ and metadata may be necessary with increasing age of the legacy data. The migration file format should be selected taking into account the balance of risk between long term accessibility versus possibility of reduced dynamic data functionality (e.g. data interrogation, trending, re-processing etc.).

605	Emphasise that GAMP 5 is a “guidance” document and not a set of requirements or a standard (a commonly held misconception).	Computerised systems should comply with regulatory requirements and associated industry-based guidance **(e.g. the GAMP® 5 Guide)** and be……..
632	Business continuity should be addressed when using outsourced services, but requiring contract content is too prescriptive and testing of the BCP may not always be necessary (e.g., low risk processes).	Business continuity arrangements should be ~~included in the contract~~ addressed and tested, as appropriate based on risk.
Grammar and typographical errors	**Something to consider during final edits:**	
30	Include (,) between complete consistent	
336	Insert (has) in “…. information that has been verified….”	
428	Include (n) in a(n) exception….	

Please add more rows if needed.