ABB Limited

Daresbury Park, Daresbury, Warrington, Cheshire, WA4 4BT, United Kingdom.
Telephone: +44 (0)1925 741111 Fax no: +44 (0)1925 741212

Facsimile

To:	Dockets Management Branch (HFA-305)
Company:	Food and Drug Administration
Fax No:	00-1-301-827-6870
From:	Per Olsson
Fax No:	+44-1925-741322
Tel No:	+44-1925-741062
Date:	09 July 2004
Pages:	This (1) + Covering letter (1) + Table (18) = 20 pages
Ref. No:	FDA/P11
Copies to:	
Subject:	**FDA Docket No 2004N-0133 Electronic Record; Electronic Signatures; Public Meeting**

Dear Sir / Madam,

Please find attached our covering letter and comments on the proposed rewording of the 21 CFR part 11 rule. We have also e-mailed these to fdadockets@oc.fda.gov, but sometimes e-mailing attachments causes delays or delivery failure, hence this fax.

Kind regards,

Per Olsson (Mr)
Principal Consultant
ABB Process Solutions

ABB Limited
Daresbury Park
Daresbury
Warrington
Cheshire
WA4 4BT
United Kingdom

Tel: +44 (0)1925 741111
Fax: +44 (0)1925 741212

Direct line: +44 (0)1925 741062
Tel Ext: 1062
Ref: FDA/P11

Dockets Management Branch (HFA-305)
Food and Drug Administration
5630 Fishers Lane
Room 1061
Rockville
MD 20852
USA

9 July 2004

Dear Sirs,

FDA Docket No 2004N-0133 Electronic Record; Electronic Signatures; Public Meeting

In accordance with the above referenced publication on April 8th 2004 in Federal register, please find attached the consolidated comments from ABB Process Solutions.

ABB Process Solutions (previously part of ABB Eutech) is a worldwide special engineering consultancy company employing some 80 people within the global ABB Ltd corporation (100,000 employees). Our key objective is to provide regulatory compliance services to the life science industry. Our clients range from the leading pharmaceutical companies and biotechnology firms to generic manufacturers and key suppliers to the industry. As such we are actively assisting our clients to achieve 21 CFR part 11 compliance based on a pragmatic risk-based model, and the application of modern computer system validation. We also provide focused training on the subject.

ABB Process Solutions plays an active role in the GAMP Forum, leading and participating in several Special Interest Groups, and providing input to the GAMP guide. One of my former colleagues, Sam Brooks, was actively involved in the drafting of the ISPE document on a "Risk-based approach to 21 CFR part 11". In general, we welcome the latest development of part 11. Last year we provided the Agency with some very detailed comments on the draft guidance, and trust that you will carefully consider our comments.

Please do not hesitate to contact me for any further information or clarification you should require. I can be contacted at either the above address or telephone number or via my e-mail per.olsson@gb.abb.com. I would welcome a discussion and look forward to hearing from you.

Yours sincerely,

Per Olsson (Mr)
Principal Consultant
Enclosed: Comments by ABB Process Solutions (18 pages)

Docket No 2004N-0133 Electronic Records; Electronic Signatures; Public Meeting
Comments by ABB Process Solutions, 3100 Daresbury Park, Warrington, WA4 4BT, United Kingdom
Contact: Per Olsson (e-mail per.olsson@gb.abb.com, telephone +44 (0)1925 741062)

ABB Ref	FDA Ref	Subject	Comment
1	A 1	Narrow scope interpretation of part 11	Please see our comment under ABB ref 2.
2	A 2	Revision of definitions - general	Presently part 11 applies to electronic records that are created, modified, maintained, archived, retrieved or distributed by a computer system, as long as the record is required under a predicate rule or submitted to the Agency. The guidance limits part 11 to electronic records that are required under predicate rules to be maintained, or are submitted to the Agency. We generally support this redefinition but with the following clarifications and restrictions. The definition of electronic record is at the heart of the problems with part 11. There are several aspects to the definition of electronic records, and we have identified five: o Limit part 11 to maintained regulated records. See ABB ref 3. o Limit part 11 to regulated records that are explicitly identified in the predicate rules. See ABB ref 4. o Limit part 11 to submitted regulated records. See ABB ref 5. o Exclude from the scope the use of electronic records for regulatory activities. See ABB ref 6. o Clarify position with regard to momentary records. See ABB ref 7. The next five comments, ABB ref 3 to ABB ref 7, deal with each of these aspects in turn. The definition of electronic record is closely linked to the question of the "real" purpose of part 11; is it as an act to regulate certain electronic records, or is it a means to improve computer validation standards? If it is the intent of the Agency to use part 11 to enforce higher standards of computer system validation, then this should be stated explicitly. At the same time, part 11 should be enforced for all GxP records. In this case, part 11 would require extensive redrafting, since there are important omissions from part 11, such as change control (configuration management), that fall within the scope of computer system validation. We must stress that we do not support this extension of intent with regard to part 11. Computer system validation standards should instead be enforced through the application and enforcement of predicate rules.

ABB Ref	FDA Ref	Subject	Comment
3	A 2	Revision of definitions – limit part 11 to maintained regulated records	By limiting the scope to "maintained" records, momentary records are excluded (see ABB ref 7). In using the word "maintained", it is implied that "archived" records are also included, since these will require to be maintained. For "generated" records modern computer validation should be used. If these records are also permanent, then they will fall under the "maintained" records definition. Similar arguments can be used for "modified", "retrieved" and "transmitted" records. For GxP records modern computer system validation should be used. It follows that 'part 11 records' are a subset of GxP records. The trustworthiness of the computer system used to generate the record, however complicated and critical the computer system or the record, is ensured through modern computer system validation. It should not be the purpose of part 11 to enforce modern computer system validation, since there are critical GxP records that do not fall under part 11. Recommendation: Redefine electronic record in the context of part 11 as: "Any combination of text, graphics, data, audio, pictorial or other information representation in digital form that is required to be maintained or submitted under applicable predicate rule(s)." This affects clauses §11.1 (b), §11.3 (6) and §11.10 (first sentence).
4	A 2	Revision of definitions - limit part 11 to regulated records that are explicitly identified in the predicate rules	The definition of electronic records that fall under part 11 is both critical and a source of confusion. We believe it would be beneficial if the Agency clarified, if by records required by predicated rule(s) is meant: (a) only those records that are explicitly identified in the predicate rule(s), or (b) all records that are required to demonstrate compliance with predicate rule(s). There is a subtle difference here. To fully demonstrate compliance often requires many additional records that are not specifically called for by the predicate rule(s). Hopefully an example may demonstrate this: A specific predicate rule clause identifies the need for a procedure (SOP) to be kept. In case (a) the SOP itself is a record. In case (b) the SOP, the associated training details, the verification of the SOP, and the management of the SOP are all records. (We are aware that some of these additional records may be required by other clauses in the predicate rule.) We strongly believe that part 11 should be limited to those records identified in (a) only. This would greatly add clarity to the rule. Records identified in (b) should instead be safe-guarded through modern computer validation, as these are not central to the part 11 legislation. Recommendation: Define records that are required by predicate rule(s) as those records that are directly identified in the predicate rule(s).

ABB Ref	FDA Ref	Subject	Comment
5	A 2	Revision of definitions – limit part 11 to submitted regulated records	Presently the rule applies to all records that are submitted, "even if such records are not specifically identified in agency regulations". This is an open-ended clause, that can extend part 11 outside the control of the submitting company, e.g. where records are submitted in response to a request for information from the Agency. Where company activities are now commonly conducted with the help of computers, and computer records are generated for almost all activities, this scope definition can potentially put unintended records and computer systems within scope of part 11. We would consider this clause to be unreasonable, as it is vague and open to abuse. It also goes against the general public request of having a better definition of "predicate rule records", and a more narrow interpretation of part 11 records. Recommendation: Redefine clause §11.1 (b) to read: "This part also applies to such regulated electronic records that are submitted to the agency." (Delete the rest of the sentence).
6	A 2	Revision of definitions - exclude from the scope the use of electronic records for regulatory activities	We support the guidance that the firm should state for each regulated record, if it is maintained in paper or electronic format. If the paper record is used for meeting predicate rule requirements, then that should be the "end of the story". The guidance states that part 11 applies to predicated electronic records that are used for regulated activities. Any electronic use of such records should be governed by modern computer system validation. It is difficult to find the rationale for applying the requirements imposed by part 11 to only certain GxP records, and two examples will illustrate this. A computer system that performs critical operations, for example controlling a vial filling machine, may have no part 11 records, but the computer system is likely to be highly critical to the integrity of the product, such as correct fill volume and error detection. Another example is a batch management system. The recipes are GMP records and are used electronically so fall under part 11. The batch record is generated electronically, but printed and signed. It is thus not used electronically and fall outside part 11. This is illogical because if anything the batch record (what happened) is more important that the recipe (what should have happened). This dilemma is best solved by restricting part 11 to its initial intent, i.e. that of allowing electronic signatures and supporting electronic records, and let computer validation deal with all other matters. Recommendation: The use of electronic records for performing regulated activities should not be within the scope of part 11. This should instead be covered by the application of modern computer system validation.

ABB Ref	FDA Ref	Subject	Comment
7	A 2	Revision of definitions – clarify position with regard to momentary records	There is no mention in the rule or guidance of momentarily stored (transient) records. It is general industry consensus that these do not fall under part 11 (please refer to GAMP), but the rule itself and its preamble does not make this clear. It would be welcome if the preamble or guidance included this clarification for completeness, as well as attempting to define a momentarily stored (transient) record. To stimulate a discussion, we have proposed some wording below. Having this additional guidance would support the case of restricting the definition of electronic records to those that are maintained. Recommendation: Add the following guidance: "Momentarily stored (transient) records that are not used for making GxP critical decisions, do not fall under part 11. It is recommended that a risk assessment should be carried out for momentarily stored records that are used for making GxP critical decisions. This risk assessment should identify how these records can be made secure. A momentarily stored record, is a record that is kept on a computer system for a brief period of time, and is not readily accessible to the user, and is then either automatically deleted, transformed or transmitted to another location or system (including being printed)."
8	A 3	Which records are required by predicate rules?	Please see our comment under ABB ref 4.

ABB Ref	FDA Ref	Subject	Comment
9	B (gen) 1	Applying a risk based approach to the whole of part 11	We agree and support the intent and general content of the guidance, which incidentally is largely in line with the approach we have adopted for several years. A risk-based pragmatic approach is essential to be able to deal with the complex issues that arise from part 11, as they apply to a range of laboratory, business and manufacturing systems of varying degree of age and sophistication. The approach to part 11 should not materially differ from that applied to modern computer system validation. It is fully understood why provisions for enforcement discretion have been made in the short term, i.e. to quickly alleviate the most cumbersome and controversial aspects of part 11. In the medium to longer term, and in the context of a risk-based approach, these concessions make less sense. We would advocate universally adopting the risk-based approach to all aspects of part 11, and the withdrawal of specific discretions. This would encourage a consistent approach, which is in harmony with current validation practices. There is no logic in applying a risk-based approach to only certain aspects of the rule. Not adopting a uniform approach to part 11 will inevitably lead to inconsistencies. Take clause §11.10(j) for development personnel as an example. Consider a well-established computer system, which has been in beneficial use for several years, as opposed to a new computer system, that hitherto is untried. In this example, having appropriate records that demonstrate competence by the development personnel, is clearly much more critical for the new computer system, compared with the well-established one. Clause §11.10(j) is presently outside the stated enforcement discretion and risk-based approach. Applying a documented, rational and credible risk-based approach to the whole rule, would ensure optimal benefits to be drawn from the application of part 11. A universal adoption of a risk-based approach would be consistent with the FDA initiative for drug enforcement in the 21st century. A piecemeal approach, with risk assessment for only certain sections of the rule, is not consistent with the FDA drug enforcement initiative. Recommendation: Withdraw the concessions of enforcement discretion to certain parts of the rule, and instead adopt universal risk-based enforcement discretion to the whole of part 11.
10	B (gen) 2	Clarification of predicate rule requirements under part 11	This is a very open question, and hence difficult to answer. It seems logical that any clarification of predicate rules, and how they relate to electronic records, should be done as part of the guidance for the particular predicate rule rather than in part 11. Part 11 is a general rule that applies across the whole of 21 CFR. Every time a predicate rule is changing, how will it be practical to revise part 11 and its guidance? Different predicate rules will have different requirements and hence potentially different solutions. It is difficult to see how part 11 can be more specific on these aspects, and it is questionable if part 11 should be more prescriptive. Again, this is most likely better dealt with by each predicate rule.

ABB Ref	FDA Ref	Subject	Comment
11	B (gen) 3	Separation between maintained and submitted records	This question has arisen as a direct result of the wide scope of part 11, and only serves to illuminate the inherent difficulties achieving compliance. Our recommendation as detailed in the comment ABB ref 5 makes no distinction between the two. A submitted record (under the ABB definition), should be subject to the same controls as maintained part 11 records (under the ABB definition).
12	B (gen) 4	Any distinction between open and closed system	Part 11 contains definitions for open and closed systems. These are suitably vague and in practice not always that easy to determine and often lead to some discussion. Interestingly, however, the rule does not impose additional controls for open systems, simply suggests encryption. The way this clause is sometimes applied in practice is, that a system that is identified as an "open" system will have additional controls added to it, and is then reclassified as "closed". Yes, you can argue about the semantics for this approach, but the end result is that threats to the system have been identified and dealt with, making the system and its records secure and trustworthy. In this context, the rule or its guidance is correct to identify potential threats posed by interconnected systems, be it through serial links, networks, intranet, web access, remote dial facilities, etc. These threats may apply to both open and closed systems. It is questionable if the current term "open system" is helpful. Take a clinical trial database as an example. This may coexist with other data on several servers. To talk of "system access" in this context may be less relevant than "record access". A separate case is the need for confidentiality, which applies to e.g. clinical records, but less often to GMP records. Confidentiality is often linked to record ownership (but not always). Another special case to consider may be outsourcing of infrastructure control and management. These cases are best dealt with in the guidance rather than in the rule itself. Recommendation: Delete the definitions for open and closed systems, and instead include in clause §11.10 that "Consideration should be taken to protect the integrity of records from potential security breaches posed by interconnected systems, such as through serial links, networks, intranet, web access, remote access facilities, etc."

ABB Ref	FDA Ref	Subject	Comment
13	B (ind) 1	Validation requirement under predicate rules	This question refers to clause §11.10 (b), but should this read clause §11.10 (a)? We have made this assumption. Systems that handle GxP records shall be validated. The main problem with clause §11.10 (a) is not the requirement that the system should be validated – this is a given – but in the statement "the ability to discern invalid or altered records". Frequently this is achieved through access and operational controls, but this is not the same. For a start, to be able to "discern invalid data" you must first define what is valid data. For data that is manually entered this may not be so difficult, but for all other data it can be a problem. The words "accuracy" and "reliability" could probably be deleted, as they can be taken to be included in the statement "consistent intended performance". On the other hand, "fitness for intended purpose" would ensure the stated specification is suitable for the given application. Further more the word "ensure" implies almost a guarantee that the system will be able to meet these requirements. This sits uncomfortably with the definition of process validation, which states "high degree of assurance". Recommendation: Reword clause §11.10 (a) to read: "Validation of systems to provide a high degree of assurance of consistent intended performance and fitness for intended purpose".

ABB Ref	FDA Ref	Subject	Comment
14	B (ind) 2	Requirements for record retention and copying	Maybe we have misunderstood this question, but find it almost impossible to answer. The requirements for the record will vary with the type of record and its intended purpose, e.g. is the Agency only interested in the record content or is also its metadata needed? There is no single answer to this question. There are two cases to be considered: (a) Electronic copies provided for the use by the Agency. (b) Electronic copies to be used for GxP activities that may affect product quality or product quality related data. In case (a) the firm should be able to demonstrate to the Agency that 'true copies' of records are provided, as these relate to reasonable information request by the Agency. This may imply a subset of record information and metadata. In case (b) the firm should be able to demonstrate to the user that 'true copies' of records are provided as these relate to the GxP critical use of such copies. Again, this may imply a subset of record information and metadata. In general we do not think that the rule should be specific with regard to specifying requirements for preserving record security and integrity. Requirements for record retention and record copying should be defined at the time of record definition. Any limitations in the ability to copy and retain records should be stated. Where these limitations are likely to directly affect GxP activities, i.e. those having a direct impact on product quality or product data, the potential impact should be assessed and approved by management (risk assessment).

ABB Ref	FDA Ref	Subject	Comment
15	B (ind) 2	Requirements for record retention and copying	The guidance does not address the, often difficult, question of when and how to preserve manifestation of electronic signatures. This was discussed in the draft guidance on electronic copies of electronic records section 5.7 (now withdrawn). Guidance on this subject would be welcome. There are two cases to be considered: (a) Electronic copies provided for the use by the Agency. (b) Electronic copies to be used for GxP activities that may affect product quality or product data. In case (a) the firm should be able to demonstrate to the Agency that 'true copies' of records are provided. Any authentication of signatures, however, could be demonstrated to the Agency on the original records. In case (b) the authentication of signatures is more critical, since the user of the signed copied record, must be able to ascertain that the record has been properly signed. Depending on the use of the copied record, e.g. for critical GxP activity or for information only, signature authentication may or may not be required. A risk assessment should determine the authentication requirement. Recommendation: Add to guidance: "Copies of electronic records should preserve meaning and context of the copied record, and, if applicable, signature manifestation. A risk assessment should determine the need for preserving signature authentication. This risk assessment should be based on the intended use of the copied electronic record and signature."
16	B (ind) 2	Requirements for record retention and copying	The guidance recommends that copied electronic records preserve content and meaning. We generally agree with this statement. There is no specific mention of audit trails, however, and some guidance on this may be beneficial. Preserving audit trails may not always be feasible. On the other hand, an audit trail would not normally be a predicate rule record, but meta data, and would therefore, from a risk-based approach, be less critical than a predicate rule record. This would justify some leeway with regards to copies of records. Recommendation: Add to guidance: "Electronic copies should preserve the audit trail data, where required to meet predicate rule requirements, or where a risk assessment deemed this as necessary."

ABB Ref	FDA Ref	Subject	Comment
17	B (ind) 3	Audit trail requirements - general	This question highlights some of the problems around the present clause. The matter of an audit trail has unfortunately taken on more importance than access controls. In many instances there has been too much emphasis on complying with the audit trail requirement, much to the detriment of other equally or more important clauses. For example, we consider access controls to be more important than audit trails from a security point of view. The audit trail records what happened, but access controls prevent unauthorised events. Curiously, part 11 contains nothing about what you should do with the audit trail, apart from keeping it, e.g. it does not state you should review it for security breaches or consistency with generated regulatory records. It misses the point why having an audit trial in the first place, and has lead to requirements from inspectors for audit trails even where data cannot be modified. Clearly, the guidance has overcome many of these problems. Recommendation: Add to part 11 or guidance the stated purpose of the audit trail, please see our comment ABB ref 18.
18	B (ind) 3	Audit trail requirements – different events	Some of the problems in dealing with audit trails, and when to apply them, stem from the premise that part 11 doesn't differentiate or define the three types of events the audit trail is intended to cover: (a) authorised scheduled events, such as entries in a batch record, or (b) authorised unscheduled events, such as modifying the software, or (b) unauthorised events, such as inadvertently changing a measured value and fraudulent changes. Item (a) should, ideally, be covered by an automated recording of the GxP critical events. This may be data that is then presented in e.g. the batch report. As an alternative, a manual recording of these events may be acceptable, i.e. a hybrid system. Item (b) is usually handled through a manual change control system, where the changes are recorded either by hand or through various electronic copies or print-outs. Item (c) is the one that is least suitable to manual records, particularly to prevent fraud. On the other hand, stringent access controls may sufficiently alleviate the risk of unauthorised changes. Recommendation: Add: "It is recommended that the risk assessment should identify how changes from authorised events (scheduled and unscheduled) and unauthorised events (advertent and inadvertent changes) can be captured. This may be achieved through a combination of various methods such as an automated electronic audit trail, application programming, access controls and procedural measures. The chosen method(s) should be commensurate with the perceived risk."

ABB Ref	FDA Ref	Subject	Comment
19	B (ind) 3	Audit trail requirements – recording of individuals	The guidance does not address the question if the identity of an individual must be recorded in the audit trail. The rule itself does not state this, but the preamble clause 72 does indicate it ("who did what"). This has ramifications on clauses §11.10 (d) and §11.10 (g), i.e. are group access controls acceptable or not? The rule is not clear on this point. We would maintain that group access controls may be appropriate, but that this depends on how tightly they are controlled and applied, how critical the computer system and application is, and the criticality of any human actions. We would welcome some guidance on this matter. Recommendation: Add: "Normally, individual access controls should be applied. Where this is not practicable to do, a risk assessment should be carried out to determine if group access controls could be used, without posing an unacceptable risk to the integrity of the maintained record."
20	B (ind) 4	Documentation controls	Clause §11.10 (k) (1) is difficult to comply with. We interpret this clause as "provide information on a need-to-know basis". For example, it is not desirable to provide an operator with information on how to program / code a system, with the potential security problems this may bring. With modern systems that have built-in help functions and web-based access this clause becomes near impossible to comply with. Clause §11.10 (k) (2) is easier to comply with but is very specific. We re-interpret this clause to mean that documentation should reflect installed software functionality and be current, consistent, correct and comprehensive. We think this is more important than having document audit trails, which are only a tool to achieve current, consistent, correct and comprehensive documentation. Terms such as software configuration, configuration management, baselines, and change control are all linked to documentation requirements. We include software in documentation in accordance with stated FDA policy that code listings should be treated as raw data. As long as it is made clear that software is included in the term "documentation", this should suffice without the need to specifically address configuration. Recommendation: Reword the whole of clause §11.10 (k) to read: "Use of appropriate controls over system documentation, including software, to render it current, consistent, correct and comprehensive, and available as required for the safe operation and maintenance of the system." Delete clauses §11.10 (k) (1) and (2).

ABB Ref	FDA Ref	Subject	Comment
21	C	Handling of security breaches	Again we are not sure we have understood the question. The question regarding handling of security breaches is asked in the context of electronic signatures. This aspect is already addressed by the rule for password signatures in clause §11.300 (d), which stipulates that there should be a system for handling security breaches. Clause §11.10 (d) is unsatisfactory insofar that no clear distinction is made with clause §11.10 (g). This problem is exacerbated by the fact that there is no preamble or guidance for clause §11.10 (d). We generally interpret this clause to deal with non-application specific access control, including physical controls. It would make sense that clause §11.300 (d) is deleted and made general for any security breach affecting electronic records or any type of electronic signature. Apart from having a method in place for dealing with security breaches, the rule should not stipulate how this method is designed as long as it can be demonstrated to work in an efficient manner. Recommendation: Delete clause §11.300 (d) and replace it with a new clause that is applicable to both electronic records and signatures. Add: "There should be a documented method in place for detecting security breaches to electronic records and signatures, and for assessing and dealing with any implications from said security breaches as far as they may affect product quality or product data. Such method shall be verified as being effective in meeting these requirements."
22	C	Linking of signatures to record	A common source of discussions and interpretation difficulties are clauses §11.50 and §11.70. The guidance does not cover them, and although the FDA notice does not specifically ask questions with regard to these clauses, we have taken the liberty to offer some suggestions. Some guidance on these two clauses would be welcome. The main source of discussion is if (and if so how) these clauses affect hybrid systems, i.e. electronic records that are printed and signed using wet ink. To stimulate this discussion, we have proposed some additional wording below. Recommendation: Add to clause §11.50: Where a hybrid system is used, then the 'time' element of clause (a)(2) does not apply. Recommendation: Add to clause §11.70: Where a hybrid system is used, it should be possible for the user of the electronic record to ascertain if the record has been signed or not. This may be achieved by marking the electronic record as signed, or by storing the signed electronic record in a dedicated location, where it cannot be mistaken for the unsigned record.

ABB Ref	FDA Ref	Subject	Comment
23	D 1	Economic ramifications of modifying part 11	The implications of any changes to part 11 depend on the nature of the changes, any provisions for compatibility with the 'old' rule, and how much work the firm has already expended on achieving part 11 compliance. Where a firm already complies with part 11 as it now stands, there should be a provision in the rule, if required, that no additional work is required by the firm to demonstrate compliance with the new part 11. With the proper wording of the new part 11, this will not be a problem, i.e. any reworded clauses should be carefully assessed for impact against the old rule wording. The main benefit of the new part 11 is that it will enable a more flexible approach and implementation. As such this should not lead to a cost penalty compared with the present situation. When rewriting part 11, it is important to recognise the good effects the rule has had in enhancing system security and user awareness. There are now many systems and applications that comply with the rule requirements, something that was not the case a few years ago. The new rule should not be reworded to the detriment of much needed improvements to computer system integrity. Any new rule will lead to a considerable demand for clarification from the Agency. It would be undesirable if new up-to-date guidance is only made available several years after the rule has been rewritten. This would lead to an unacceptable situation for both firms and inspectors, and is likely to lead to further delays in bringing systems into compliance. Recommendation: Retain the positive influence part 11 has had on computer system integrity when rewriting the rule. Issue up-to-date guidance at the same time as the rule is reissued.
24	D 2	Clarification of predicate records	This question is closely linked to question A2, please see our comment under ABB ref 4. It is difficult to see how part 11 can define the required predicate records. This should be done by each predicate rule. There should not be a need to refer to part 11 to work out which predicate records are required.

ABB Ref	FDA Ref	Subject	Comment
25	D 2	Clarification of predicate signatures	More of a problem than identifying predicate records can be to identify predicate signatures. The predicate rules frequently imply a signature through the use of words, such as "approved", "reviewed" or even "verified". For consistency of understanding, it would be helpful if the Agency better defined instances of signatures in predicate rules, but it is difficult to see how this could be done in part 11. The rule does not explore the often fundamental difference of use between a wet signature and an electronic signature. Nor is there any guidance on this pivotal subject. Consider the purpose of an electronic signature; we would maintain that it is not always the same as a wet signature! In the 'paper world' we often use initials or signatures to simply state that an event has taken place. In the 'electronic world' this is not required, since the computer system will know what is taking place through the application of access controls and event reporting. An example will hopefully illustrate this. In a manual GMP plant, the operator will manually open a valve and record by means of signature on the paper batch record that he/she has opened the valve. In an automated plant, the operator will log on to the system and open the valve via the keyboard. No signature is needed, since the batch report will now contain who operated the valve, and will also state if there was an error in opening the valve. Despite this solution not using a signature, the overall security and reporting is superior compared to the manual system. There is no case to be made for also having an electronic signature, unless the opening of the valve was identified in predicate rules as an event requiring a signature (highly unlikely to be the case). In general, an electronic signature should only be applied as "an act of accepting responsibility". Using this definition, it is possible to separate out instances of what may look like a signature, but is used for security reasons, for example as log on or for initiating an assay. Another aspect is that it is generally desirable to keep the number of signature events as low as possible. The more frequently a signature is applied, be it on paper or electronically, the higher the risk that it is debased. There are too many examples where signatures are applied without much thought. Using a password as signature only increases this risk. The fewer signature events, the more likely the person applying the signature will take care in executing it and consider the responsibilities carried by the signature. Recommendation: Include guidance, based on the discussion above, to clearly state the difference between applying an electronic signature as (1) an act of accepting responsibility and (2) as part of a security related event. State that the use of computer systems may make many traditional signature events not required, provided the computer system has been appropriately configured for access controls and event reporting.

ABB Ref	FDA Ref	Subject	Comment
26	D 3	Does part 11 discourage innovation	Any innovation carries a risk, which must be weighed against the hoped for benefits. Increased regulatory risk applies to any case where an untried method, technical solution or approach is used. This risk increase can be alleviated in three ways by the Agency: (a) By having regulation that does not stifle innovation by being too prescriptive. This is the problem with part 11, e.g. it stipulates that there must be an automatic audit trail, even if records cannot be easily modified and the audit trail would serve little benefit. (b) By enforcing regulation in a pragmatic and overall risk reducing manner. This entails inspectors to look beyond the wording of the regulation, and instead apply enforcement discretion across the board based on a risk based approach. See our comment under ABB ref 9. (c) By applying consistent enforcement, both across the FDA regulations, but also in coherence with regulatory bodies from other countries, most noteworthy the EMEA. Aligning part 11 with EU regulation and PIC/S would help.
27	D 4	How can part 11 promote innovation	Innovation is probably mostly driven by economical and technical factors rather than regulatory ones. Where regulatory factors do drive innovation, it tends to be at a (considerable) cost to the firm. The main purpose of the regulation should thus be not to stifle innovation, please see our comment under ABB ref 26.
28	D 5	Details of risk-based approaches as the apply to part 11	The part 11 guidance makes numerous references to a risk-based approach, without defining what is meant or giving illustrating examples of how these could be carried out. This carries a risk (no pun intended) as different firms will apply varying degrees of rigour to the risk assessment. FDA guidance on what is meant by a risk-based approach and examples of how this can be applied would be welcome. Such guidance should not be restricted to part 11, however, as it sits at the heart of the new regulatory approach to drug inspection announced two years ago. The development of such guidance can, and should, therefore be conducted separately from part 11. Furthermore, such guidance should be pragmatic, otherwise it will severely undermine the intent of the new part 11 and guidance. In this context it is worthwhile noting the work being undertaken by ISPE/GAMP, in particular the draft guide to "risk management approach to compliant electronic records and signatures". It is desirable that any guidance and clarification is provided in a coordinated and consistent way with that being produced by recognised industry bodies.

ABB Ref	FDA Ref	Subject	Comment
29	D 6	Enforcement discretion of legacy systems	In many cases, systems that were operational on 20 August 1997 have not remained unchanged. The guidance does not define to what extent a system must not change, for it to be still classified as a legacy system. Guidance on this subject would be welcome. We would prefer, however, that the clause on legacy systems is withdrawn, and that a risk-based approach and enforcement discretion is applied to all aspects of part 11. Please refer to our comment under ABB ref 9. Under a risk-based approach there is no logical reason for treating systems differently because of some arbitrary date. Retrospective legislation should as a rule be avoided, but the present rule already applies retrospectively. Legacy systems are now seven years old, so economical factors are increasingly forcing the replacement of these systems. A risk-based pragmatic approach would assess if these systems still posed a risk to public health, and on that basis should the systems be made to comply. Recommendation: Add to guidance: "Legacy systems that have been subjected to material functional changes, that significantly impact either product quality or product data or both, will from an inspection point of view not be treated as legacy systems." Or, preferably, apply enforcement discretion to all systems irrespective of their age.
30	D 7	Record conversion	Record conversion is primarily an aspect of the record archiving requirement. There is presently no readily available commercial solution to long-term secure storage and retrieval of electronic records. This is a fast moving area, and is not well suited for inclusion in the rule itself. It is also contradictory to the demands to make the rule less specific and prescriptive. Some guidance on the subject would be beneficial, however. The ISPE/GAMP have a special interest group, SIG, addressing electronic data archiving. Input from the FDA to this SIG as well as to other guidance documents presently being prepared by industry bodies would be welcome.

ABB Ref	FDA Ref	Subject	Comment
31	D 8	What is the impact of new technology on part 11?	A difficult question to answer! If the rule is reworded to become less specific and prescriptive, then this should become less of a problem. The current rule contains many requirements for electronic signatures using identity and password. This is unfortunate, as it can give the incorrect impression that the Agency almost condone this type of signature. A signature employing identity and password only, is probably the most undesirable one based on its poor security and low recognition of being a signature and not a security measure. Making the rule wording concentrate on the purpose of the requirements, rather than their realisation, would help. We have already pointed out the discrepancy over audit trails, where the current rule is very prescriptive, but does not cover at all the purpose of the audit trail, and any requirements for using it to verify security breaches and/or integrity of regulated records and signatures. Another example is electronic signatures. Rather than stipulating more detailed controls for these, the rule should emphasise what makes a signature unique, as opposed to a security measure such as logging in. A signature is applied for a particular reason, most commonly to accept responsibility for an activity or event. That reason must be made very clear and distinguishable from security measures, e.g. by being clearly identified in an operations SOP. This distinction is often muddled for identity & password solutions (even the preamble to the rule incorrectly in our view states that the first system log-on is a signature event). Please refer also to our comment under ABB ref 25.

ABB Ref	FDA Ref	Subject	Comment
32	D 8	What is the impact of new technology on part 11 – password ageing	Another example of where the rule is too detailed and prescriptive, rather than concentrating on the principles, and this may lead to problems, is the case of password ageing. In our opinion password ageing may not always constitute a security threat, and should therefore not be made compulsory. In today's society passwords are a reality. As individuals we use passwords for many diverse systems and situations, e.g. network access, application packages access, bank cards, TV access codes, door security, burglar alarm systems, etc., etc. To remember all these passwords can be difficult, especially as they are not all configurable by the user. Introducing password ageing for perhaps many GxP systems would substantially add to this burden. This may result in people writing down the passwords (we are after all human), something that would increase the security threat. The use of unsuitable passwords, such as year of birth, favourite football or baseball team, your name, etc., are likely to pose a greater threat to security than password ageing. Where a password has been compromised or is suspected of having been compromised or even could have been compromised, disabling the password is the correct action. Recommendation: Reword clause §11.300 (b): "Ensuring that identification code and password issuances are periodically checked. Where the possibility exists that these could have been compromised, they should be recalled and changed. Passwords should, where practicable, conform to industry good practice, that is commensurate with the potential risk posed by compromised passwords".