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

14 April 2003

Dear Sirs,

Docket No 03D-0060 Draft Guidance for Industry on "Part 11, Electronic Records; Electronic Signatures – Scope and Application"

In accordance with the above referenced publication on 25 February 2003 in the Federal Register, please find attached the consolidated comments from ABB Eutech Process Solutions Ltd.

ABB Eutech Process Solutions Ltd is a worldwide engineering consultancy company employing some 500 people within the global ABB Ltd corporation. We provide amongst other things 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. We are actively assisting our clients to achieve 21 CFR Part 11 compliance, based on a risk-based model, and the application of modern computer system validation.

ABB Eutech Process Solutions Ltd plays an active role in the GAMP Forum, leading the Supplier Forum and chairing several Special Interest Groups. One of my 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 In general, we welcome the draft guidance, and hope that you will consider our comments.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 e-mail per.olsson@gb.abb.com. I look forward to hearing from you.

Yours sincerely,

Per Olsson (Mr)
Principal Consultant

Enclosed: Comments by ABB Eutech Process Solutions Ltd (8 pages)

03D-0060 ABB Limited C 9

Docket No 03D-0060 Draft Guidance for Industry on "Part 11, Electronic Records; Electronic Signatures – Scope and Application"
Comments by ABB Eutech Process Solutions Ltd, 3100 Daresbury Park, Warrington, WA4 4BT, United Kingdom
Contact: Per Olsson (e-mail per.olsson@gb.abb.com, telephone +44 (0)1925 741062)

Item	Lines	Subject	Comment
1	None	General content	We agree and support the intent and general content of this draft guidance, which incidentally is largely in line with the approach we have adopted for several years. 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, a risk-based pragmatic approach is essential. The approach to Part 11 should not materially differ to that applied to modern computer system validation. We therefore warmly welcome this new FDA initiative. Recommendation: Implement the draft guidance, but with consideration to the comments given below.
2	120-123 125-135	Enforcement discretion of certain parts of the rule	It is fully understood why this provision is 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. 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. 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. 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.

Item	Lines	Subject	Comment
3	149-156	Definition of electronic record	The definition of electronic record is at the heart of the problems with Part 11. 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 draft guidance appears to limit Part 11 to electronic records, that are required under predicate rules to be maintained, or are submitted to the Agency. We wholeheartedly support this redefinition. Part 11 should only apply to the electronic regulated or submitted records. For GxP records modern computer system validation should be used. It follows that 'Part 11 records' are a subset of GxP records. That a computer system is incidental in generating a 'Part 11 record' should be immaterial, if that record is maintained and submitted in paper form. 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. 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, such as change control (configuration management), that fall within the scope of computer system validation. 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)." Please refer also to items 4 and 6 below.

Item	Lines	Subject	Comment
4	149-156	Definition of electronic record	This comment is closely linked to item 3 above and item 6 below. The definition of electronic record that falls 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, which 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) Recommendation: Define records that are required by predicate rule(s) as those records that are directly identified in the predicate rule(s).
5	151-156	Incidental use of computer systems	This clarification is welcomed, as it would clearly remove Word processors that are used for producing documents, which are printed and signed by hand, and maintained and distributed in paper format. On the other hand, the word "incidental" is open to interpretation, and some examples would greatly enhance the understanding. For example, is a spreadsheet that contains formulas and perhaps macros incidental? Is a distributed control system (DCS) used for generating batch records incidental? Is a database that holds data that is subsequently used in a printed report incidental? Recommendation: Include examples of incidental and non-incidental systems. Or, preferably, consider excluding these records in the definition of scope of Part 11, as we suggest above (item 3).

Item	Lines	Subject	Comment
6	168-183	Electronic records that are used for GxP critical operations	This comment is closely linked to items 3 and 4 above. We support the draft 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". 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. 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. The draft guidance states that Part 11 applies to predicated electronic records that are used for regulated activities. Recommendation: Limit Part 11 scope to electronic records that are maintained under predicate rule(s) or submitted to the Agency. Their use for performing regulated activities should not be within the scope of Part 11, but instead covered by the application of modern computer system validation.
7	168-183	Momentary records	There is no mention in the draft 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 draft 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. Recommendation: Add: "Momentarily stored (transient) records that are not used for making GxP critical decisions, do not fall under Part 11. 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	191-192	When is a signature a signature?	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. Recommendation: Reword the sentence to read "Electronic signatures that are intended to be the equivalent of handwritten signatures, initials and other instances of signings (such as 'approved', 'reviewed' and in some cases 'verified') required by predicate rules."

Item	Lines	Subject	Comment
9	191-192	Linking of signatures to records	A common source of discussions and interpretation difficulties are clauses §11.50 and §11.70. Some guidance on these two clauses is therefore 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 wording below. Recommendation: Clause §11.50: Where a hybrid system is used, then 'time' element of clause (a)(2) does not apply. Recommendation: 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.
10	191-192	Guidance on electronic signatures	The draft guidance contains no guidance on the implementation and use of electronic signatures. It is true to say that clauses §11.100, §11.200 and §11.300 have raised far less interpretation issues than the rest of Part 11, but some guidance would be welcome. To stimulate this discussion, we have made one proposed wording below in relation to 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: 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.

Item	Lines	Subject	Comment
11	218-222	Recording of individuals in audit trails	The draft 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."
12	224-232	Audit trails	This clarification is welcomed, as it removes many uncertainties and sources of much remediation work, some of which may be better directed to other higher risk elements. 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. Item (a) should, ideally, be covered by an automated recording of the GxP critical events. This may be data that is then presented in 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 various methods such as an automated electronic audit trail, application programming, and procedural measures. The chosen method should be commensurate with the perceived risk."

Item	Lines	Subject	Comment
13	236-240	When is a legacy system subject to enforcement discretion?	In many cases, systems that were operational on 20 August 1997 have not remained unchanged. The draft 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 item 2 above, which makes a similar point. Recommendation: Add: "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, consider applying enforcement discretion to all systems, as suggested above (item 2).
14	256-257	Copies of records to preserve content and meaning relating to electronic signature	The draft 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: "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."

Item	Lines	Subject	Comment
15	256-257	Copies of records to preserve content and meaning	The draft guidance recommends that copied electronic records preserve content and meaning. We 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: "Electronic copies should preserve the audit trail data, where required to meet predicate rule requirements, or where a risk assessment deemed this as necessary."
16	257-259	Record search facility for copies of records	The words "technically feasible" in this sentence may lead to unjustifiable high costs, if it is interpreted as 'if at all possible'. It may also imply that the firm should provide the Agency with the required software licences, search tools and application software. It could be argued that this sentence could be removed from the draft guidance, since the predicate rules themselves provide some useful guidance on how records should be searched, e.g. 21 CFR 58 §190 (b) & (e). Alternatively, the expression "technically feasible" could be reworded. Recommendation: Remove this sentence, as guidance is already provided by the predicate rules. Alternatively, replace "technically feasible" with "practicable to do so".