



Regulatory Subgroup

Electronic Data Management Forum

Regulatory Subgroup

Summary of Outputs

December 2001





1. BACKGROUND

Sources

This document draws upon EDM Forum members experiences and understanding of regulatory authority positions on use of EDC trials for submissions. The document content is unconfirmed and will be updated as new information becomes available. This working document is made available 'as is' subject to the following disclaimer in accordance with the groups information sharing policy.

Disclaimer

The contents of this document are based upon the experience and understanding of members of the EDM Forum. As such they represent historical experiences and current understandings within the unique environment of member companies. The information presented in this document is therefore presented as an aid to understanding the uptake of EDC and for maximizing the success of EDC and needs to be interpreted in the light of your own internal environment, needs and experience. The content has not been confirmed with relevant authorities.

Access to Further Information

EDM Forum members are available to provide further guidance and information. Please contact us via Email describing your need and we will put you in touch with a member company that has handled a similar experience.

Providing Feedback

Feedback via:

- o edmforum@edmforum.com

2. DOCUMENTS THAT ARE REQUIRED READING BEFORE EMBARKING ON EDC TRIALS



FDA Regulations/Guidance Documents

1. FDA, 21 Code of Federal Regulations Part 11, *Electronic Records; Electronic Signatures; Final Rule*. Federal Register Vol. 62, No. 54, 13429, March 20, 1997. (U.S. Government Printing Office, Washington, DC) http://www.fda.gov/ora/compliance_ref/part11/
2. FDA, *Guidance for Industry: Computerized Systems Used in Clinical Trials*, April 1999. http://www.fda.gov/ora/compliance_ref/bimo/ffinalcct.pdf
3. The Gold Sheet (Vol. 34, No.10, October 2000) <http://www.fdcreports.com/goldout.shtml>
4. FDA Compliance Policy Guide: Section 160.850 Enforcement Policy: 21 CFR Part 11; Electronic Records; Electronic Signatures (CPG 7153.17)
5. GCP (FDA and ICH) for Predicate Rules

Documents are Available At:

FDA Documents are available at: <http://www.fda.gov>

EMA documents available at: <http://www.eudra.org>

ICH documents available at <http://www.ifpma.org>

Other Documents that may be of Interest:

European Data Protection Act, UK HMSO web sites

<http://www.dataprotection.gov.uk/eurotalk.htm>

<http://www.legislation.hmsso.gov.uk/acts/acts1998/19980029.htm>

3. OVERVIEW OF HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Overview: Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information. In the past, family doctors and other health care providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving gaps in the protection of patients' privacy and confidentiality.



Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The law included provisions designed to save money for health care businesses by encouraging electronic transactions, but it also required new safeguards to protect the security and confidentiality of that information. The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. When Congress did not enact such legislation after three years, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. During an extended comment period, HHS received more than 52,000 communications from the public. In December 2000, HHS issued a final rule that made significant changes in order to address issues raised by the comments. To ensure that the provisions of the final rule would protect patients' privacy without creating unanticipated consequences that might harm patients' access to care or quality of care, HHS Secretary Tommy G. Thompson opened the final rule for comment for 30 days. After that comment period, President Bush and Secretary Thompson decided to allow the rule to take effect on April 14, 2001, as scheduled, and make appropriate changes in the next year to clarify the requirements and correct potential problems that could threaten access to or quality of care. Secretary Thompson's statement on this issue is available at <http://www.hhs.gov/news/press/2001pres/20010412.html>.

COMPLIANCE SCHEDULE

The final rule took effect on April 14, 2001. As required by the HIPAA law, most covered entities have two full years - until April 14, 2003 - to comply with the final rule's provisions. The law gives HHS the authority to make appropriate changes to the rule prior to the compliance date.

COVERED ENTITIES

As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

INFORMATION PROTECTED

All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule.

CONSUMER CONTROL OVER HEALTH INFORMATION

Under the final rule, patients will have significant new rights to understand and control how their health information is used.



Regulatory Subgroup

- Patient education on privacy protections. Providers and health plans will be required to give patients a clear written explanation of how the covered entity may use and disclose their health information.
- Ensuring patient access to their medical records. Patients will be able to see and get copies of their records, and request amendments. In addition, a history of non-routine disclosures must be made accessible to patients.
- Receiving patient consent before information is released. Health care providers who see patients will be required to obtain patient consent before sharing their information for treatment, payment, and health care operations. In addition, separate patient authorization must be obtained for non-routine disclosures and most non-health care purposes. Patients will have the right to request restrictions on the uses and disclosures of their information.
- Providing recourse if privacy protections are violated. People will have the right to file a formal complaint with a covered provider or health plan, or with HHS, about violations of the provisions of this rule or the policies and procedures of the covered entity.

BOUNDARIES ON MEDICAL RECORD USE AND RELEASE

With few exceptions, such as appropriate law enforcement needs, an individual's health information may only be used for health purposes.

- Ensuring that health information is not used for non-health purposes. Health information covered by the rule generally may not be used for purposes not related to health care - such as disclosures to employers to make personnel decisions, or to financial institutions - without explicit authorization from the individual.
- Providing the minimum amount of information necessary. In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of medical records for treatment purposes because physicians, specialists, and other providers need access to the full record to provide quality care.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

The final rule establishes the privacy safeguard standards that covered entities must meet, but it gives covered entities the flexibility to design their own policies and procedures to meet those standards. The requirements are flexible and scalable to account for the nature of each entity's business, and its size and resources. Covered entities generally will have to:

- Adopt written privacy procedures. These include who has access to protected information, how it will be used within the entity, and when the information may be disclosed. Covered entities will also need to take steps to ensure that their business associates protect the privacy of health information.



- Train employees and designate a privacy officer. Covered entities will need to train their employees in their privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORDS USE AND RELEASE

In HIPAA, Congress provided penalties for covered entities that misuse personal health information.

- Civil penalties. Health plans, providers and clearinghouses that violate these standards will be subject to civil liability. Civil money penalties are \$100 per violation, up to \$25,000 per person, per year for each requirement or prohibition violated.
- Federal criminal penalties. Under HIPAA, Congress also established criminal penalties for knowingly violating patient privacy. Criminal penalties are up to \$50,000 and one year in prison for obtaining or disclosing protected health information; up to \$100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to \$250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

BALANCING PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

In limited circumstances, the final rule permits - but does not require - covered entities to continue certain existing disclosures of health information without individual authorization for specific public responsibilities.

These permitted disclosures include: emergency circumstances; identification of the body of a deceased person, or the cause of death; public health needs; research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board; oversight of the health care system; judicial and administrative proceedings; limited law enforcement activities; and activities related to national defense and security.

All of these disclosures could occur today under existing laws and regulations, although the privacy rule generally establishes new safeguards and limits. If there is no other law requiring that information be disclosed, covered entities will use their professional judgments to decide whether to disclose any information, reflecting their own policies and ethical principles.

SPECIAL PROTECTION FOR PSYCHOTHERAPY NOTES

Psychotherapy notes (used only by a psychotherapist) are held to a higher standard of protection because they are not part of the medical record and are never intended to be shared with anyone else. All other personal health information is considered to be sensitive and protected consistently under this rule.

EQUIVALENT REQUIREMENTS FOR GOVERNMENT ENTITIES

The provisions of the final rule generally apply equally to private sector and public sector entities. For example, both private hospitals and



government medical units have to comply with the full range of requirements, such as providing notice, access rights and requiring consent for routine uses.

COST OF IMPLEMENTATION

The final rule projected the implementation costs at \$17.6 billion over 10 years - a figure more than offset by the \$29.9 billion in projected savings under the final electronic transactions regulation issued in August 2000.

PRESERVING EXISTING, STRONG STATE CONFIDENTIALITY LAWS

As required by the HIPAA law itself, stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule will set a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information, the final rule does not preempt these mandates.

COMPLIANCE AND ENFORCEMENT

The final rule will be enforced by the HHS Office for Civil Rights (OCR). Before covered entities must comply with the rule, OCR will provide assistance to providers, plans and health clearinghouses in meeting the requirements of the regulation.

A Web site on the new regulation is available at <http://www.hhs.gov/ocr/hipaa/>.

4. FREQUENTLY ASKED QUESTIONS

Item	Comments
Passwords	<p>A password should be changed on a regular interval. But by doing so many people will write the password on a piece of paper and hide it near the computer. If you are allowed not to change your password, the password will not be written down anywhere. This is a safer routine than changing the password.</p> <p><i>We came to the conclusion that the authorities never will give up this rule. To avoid that the password is written down on paper, a good idea is to let the people change their passwords themselves on a regular basis and set the password they want.</i></p> <p><i>Biological passwords are the future – iris scan, finger prints or similar – once they become cheaper and more reliable. In the meantime the pin number solution may prove an alternative. 4 digits are a bit short, but it is possible to have a fixed password string (let the user chose this) and add the pin code. This can then be incremented on a monthly basis</i></p>



Regulatory Subgroup

	<p><i>to produce a new password. If the user forgets the numeric piece then it is easy for them to calculate the password given the first text piece and adding the pin plus 1 for each month the trial has been running.</i></p>
Training	<p>The person that has been trained on a system, should that person sign the paper where it's stated that he's got the training? Is there a guideline/rule for if a CV has to be updated on a regular interval?</p> <p><i>For some of us the diploma is signed both by the trainer and the trained. But is this necessary? Must the investigator sign it? Do we have to have a diploma for the investigator or is it enough that we document his training, for example, in an Excel spreadsheet?</i></p> <p><i>For our monitors and ourselves: Most of us update our job descriptions and CV's once in a while. But we don't know if we must update them on a regular interval.</i></p> <p><i>Training could be given to the investigator via a Computer based Training course (although the CRA should/could be on hand to help). The whole process should have an automatic self-documenting feature where CRA and investigator names and signatures are entered or captured and this becomes part of the audit trail. Going a stage further the program should test the investigator with the actual protocol being used and record the fact that the investigator got a pass rate of >90% or similar. If they fail then they cannot proceed with patient enrolment. The system could even re-test on a regular basis if need be, or make the investigator aware of new information (changed eCRF, new instructions etc).</i></p> <p><i>How should the training be documented? Must the trained person sign? Is a diploma/certificate enough? Must the edc-training be documented separately or is it enough to have a common study training documentation?</i></p> <p><i>The GAMP document provides good guidance here - it indicates that it is nice to have documentation but not required?</i></p>
Electronic signatures	<p>What does it mean? If the investigators username and password is saved together with the "signed" data electronically, is that an electronic signature?</p> <p><i>We were pretty sure about that if the investigator login with a username and password to the application, then it should be enough to "sign" the data with his username OR password, not both. The software must provide the mechanism to lock the signature and signature information (date/time etc) with the electronic record.</i></p>



Regulatory Subgroup

	<p><i>The guidelines clearly say this. There are some interesting issues to be aware of: Firstly you must register with the FDA that you are going to use E-signatures as equivalent to signatures. You must ensure that the e-signatures is linked to the electronic data in a way that cannot be changed to falsify records, and both components of the e-signatures are required for logging on, but only one part (the FDA calls them components) is required subsequently. We do not think just using the username is particularly safe – since this may be easy to guess – but the FDA does not say this. However it is important to be able to lock up the terminal should the investigator wander away from the PC to prevent others entering or tampering with e-data.</i></p>
Security of data	<p>What's the level of security of data? How much security must be put in place? How should you protect a laptop on site?</p> <p><i>For an off-line system the same rules must apply as for an in-house database-system. That is, you must protect it in the same way as you do for you laptops/PC's in-house. Both for theft and unauthorised access. For an on-line system it comes down to the security of transmission. If the transmission is not encrypted then it's "official" and can be read by anyone. It must be encrypted in some way. 128 Bit is the most secure - but what about countries that do not permit 128 bit encryption? In France, the law which forbids encryption, has been changed in 1996 and authorises encryption with keys up to 128 bit, but in other countries this may not be allowed – you may have to have different encryption levels for different countries to avoid breaking the law – 56bit encryption is almost universally allowed. If you look at keeping electronic records secure, then you need to address the physical, logical and procedural security at investigator and the sponsor site. This includes measures taken to protect data uploads – whether these are internet or floppy disks in the post! The FDA is concerned with maintaining confidentiality and attribution of records to protect patient and investigator. The Sponsor is interested in maintaining intellectual property, but the methods are the same. Secondly people talk about the security of the paper process – which is accepted but often much lower. We agreed with some of this – but think we should still always be looking to improve the process and provide maximum security and confidentiality.</i></p>



Regulatory Subgroup

Archiving	<p>Are the same rules applicable for paper archiving and electronic archiving?</p> <p><i>The same rules apply for electronic archiving as for paper archiving. The data should be kept as long as the duration of the drug. But there are some problems involved. In which format should we save the data? ASCII seems to be the most transportable format. But most of the data is today stored in Oracle databases. How about accessing the data when new versions cannot read old data? The investigator should have a certified copy! But what is that? Could it be a CD-ROM? But the investigators are not used to handle CD-ROM's!</i></p> <p><i>The FDA is currently reviewing this area – it is believed they are not particularly happy with a CD-Rom of pdf files – they want the data in its original format so it is possible to see the whole audit trail and maintain accessibility. We are watching this develop right now and there are many discussions taking place with the FDA and EDC companies – see accompanying document recently produced by Datatrak and published on the FDA website(attached).</i></p>
Audit trail	<p>When to start the audit trail? Should the first entered value in a field be in the audit trail? Should there be an audit trail on data from other paper or electronic sources that is loaded or feed into the main system?</p> <p><i>For on-line systems where you enter all data on a page and then press submit there is no possibility to have an audit trail for changes done to the data before you press submit. But if this is compared to paper then you can have an audit trail by crossing out the first entered value. So how about that? Part 11 is clear about this: You don't need to have an audit trail on data changed before pressing submit. See page 35 in "A comparison of the proposed rule and final rule for 21 CFR part 11"</i></p> <p><i>If the value first is recorded on a tag from a heart-lung machine, then transferred to a yellow sticker, then transferred to a paper-CRF and then entered into a on-line laptop, should there be an audit trail of all this? Part 11 is not clear about this, I think. See page 35-36 in the same document.</i></p> <p><i>The first time data is recorded on durable media is the source data. This can be both paper or electronically. So the tag from the heart-lung machine is the source data and this should be compared to the value in the database.</i></p> <p><i>The FDA at least is pretty clear again – in the Guidelines for Conducting Trials on computer based systems. The audit trail must start when the data is first committed to 'durable media'. The durable media could be paper, it could be a hard disk or a smart card. Computer memory (or the investigators memory for that matter) is not durable media and does not count. So paper and electronic are the same – see also Datatrak document mentioned above.</i></p>



Regulatory Subgroup

Third party products	<p>Who will do what testing? Both on first version and on new bugfixes/versions.</p> <p><i>In short: The vendor tests that the product is built and works according to the specifications. The customer tests that the product works in their environment and according to the specifications.</i></p> <p><i>100% QC = less validation required (theoretically none!)</i> <i><100% QC = more validation</i> <i>On-line = rather straightforward validation</i> <i>Offline = more complex validation process</i></p> <p><i>Validation guidelines are very clear. You must have confidence in any computer system that you build to handle regulated data.</i></p> <p><i>Hence if you perform 100% QC of data you are completely confident in the computer system, if you perform 0% QC you have no confidence. Validation replaces the QC process to demonstrate why you have confidence in a system without the need for 100% QC. This includes the standard elements of the Software Development Life Cycle (SDLC) from design, programming, implementation, testing, and review. If you purchase a 3rd party system you just outsource some of these elements – but the <u>responsibility</u> does not leave you. Therefore you MUST check that a vendor does all these elements and documents this fact. When you install any system in a production process you still have testing and acceptance criteria to follow. This may be more work for a system you have developed yourself (you will have to create all these), and less for a system you buy (the vendor may have done some of this work for you). Either way you must review the criteria, the results and the decision to go live with a system.</i></p>
Transfer of data	<p>All data sent via Internet must be encrypted but what else is required to ensure safe transfer of data?.</p> <p><i>There must also be a control in place to check that what is sent, really is the same that comes through. Handshaking solves this?</i></p> <p><i>Again there are two issues – data confidentiality – can other people read investigator or patient information, and integrity – is all the data received and attributable to the investigator/patient.</i></p> <p><i>Any information sent through the internet without encryption and a security notice is treated as published. You may as well send the data to ‘The Times’ newspaper! We must keep it secure (and demonstrate this for the audit trail)</i></p>



Regulatory Subgroup

	<p><i>We must also be confident data is not lost in transmission. We must do either 100% QC, or some transmission validation, or we must acknowledge all data received with a message to the investigator.</i></p> <p><i>Can we be sure we did not lose any information during transmission? Some of this is validation, some may be in the EDC application design.</i></p>
What is a guideline?	<p>Do we have to follow it? Do these become rules in a few years?</p> <p><i>We have to follow the rules of course. But we need to know if the guidelines are just guidelines that we can follow if we want to and don't follow them if we think we have a better way to do it. But if the guidelines are to become rules in a few years then we must build our systems so that they apply to the guidelines.</i></p> <p><i>The FDA clearly says a Guideline document does not 'replace' any rule, and the rule is the definitive wording. A guideline is meant to be a helpful document to explain the rule if this itself is complicated or requires explanation. It makes common sense to follow both Rules and Guidelines, but be aware that the Ruling is the definitive statement. Here is an example that has been known to highlight an apparent discrepancy between rule and guideline – but is not actually the case!:</i></p> <p><i>According to "Guidance for industry, Computerized systems used in clinical Trials", in section IIIH, you must give a reason for a change "Documentation should include who made the changes, when and WHY they were made". In CRF21, Part 11 page 37 in "A comparison of the proposed rule and final rule" it says: "The agency does not believe part 11 needs to require recording the reason for record changes because such a requirement, when needed, is already in place in existing regulations that pertain to the records themselves.</i></p>
Which guidelines, data protection	<p>FDA – Part 11, Computerized systems used in clinical trials EMA – 4.9 553 519 ICH –Data Protection laws? Japan – Own Data protection laws What if the guidelines/rules don't match? Which one to follow? See 6.1, 6.2.4 - 6.2.6 in Nice meeting minutes.</p>



Regulatory Subgroup

	<p><i>We are not sure about if there are some rules/guidelines that don't match. But to be on the safe side it's better to follow the FDA rules/guidelines since they are stricter.</i></p> <p><i>At an EDC conference last week it was clearly stated that there is NO conflict between any of these. The FDA is generally the strictest, but you must really ensure you are following all legislation for ALL the agencies you intend to present you data to.</i></p>
Audit trail	<p>Before submit of data? What if you enter data to a field and change that to another value before you have stored the data /sent it to the sponsor. Should that be audit trailed?</p> <p><i>See item 6.</i></p> <p><i>If it is saved to durable media it must be audit trailed.</i></p>
Reason for change	<p>We don't want it! This is just another text component that will fill our databases with a lot of text. For what use? What if the investigator has given an invalid reason? Should we take our time to find the valid reason?</p> <p>What is the background to the 'reason for change'.</p> <p><i>Let's say that we must use this reason for change. Can we then use drop-down lists were the reasons are pre-defined?</i></p> <p><i>And what about an alternative as "Data correction"?</i></p> <p><i>If we collect data it must be accurate data – should we make efforts to ensure this data is correct? How detailed must it be? Should it be explicit (drop down) or implicit?</i></p> <p>Has anyone been audited on 'reason for change'?</p> <p><i>There are many questions about reason for change – but it was felt that the FDA was not likely to change this in the short term. People do use a drop down list for Reason for change to make this easier to deal with – so long as there is an 'Other' column were the investigator can supply a different answer from the given drop down list this is OK.</i></p>
Version control	<p>When to start version control? Should the version control be in place for the version set in production or for the different beta releases before the final version?</p>



Regulatory Subgroup

	<p><i>To document the development of the system you should save all the different versions. But for the sake of the clinical data it's enough to save the version that goes into production. So you will end up with being forced to save all versions.</i></p>
In-house developed system	<p>How about validation of "small" third-party products included in the main system? Who's responsible for the validation?</p> <p><i>The same as in item 7.</i></p>
Documentation/validation	<p>How far do we need to go with validation? Do we validate each PC, the internet? For example if you create a shortcut, on the desktop, on a PC on site for the investigator to access an commercial, validated, application, how much documentation/validation must be in place for this shortcut?</p> <p><i>It is part of the validation process. If the shortcut is created manually then 100% QC is required (it should be tested and documented). If it is created by a program then validation of the process if required. Again the process could be self-documenting if the investigator first gains access while the CRA is teaching them.</i></p>

5. DATATRAK PRESS RELEASE

Company Press Release

Audit Trail Analysis by DATATRAK International Posted on FDA Web Site



Broader dissemination of this White Paper can serve as important background for all sponsors considering the use of EDC in clinical trials.

Cleveland, August 23, 2001 - DATATRAK International, Inc. (Nasdaq: “[DATA](#)”), the leading and most experienced Application Service Provider (ASP) in the Electronic Data Capture (EDC) industry, today announced that its recent White Paper involving a comparative analysis of audit trails with various EDC platforms in conjunction with the existing predicate rules of Good Clinical Practices (GCPs), has been posted on a public web site of the Food and Drug Administration (FDA). This web site is the FDA’s public docket on audit trail guidance for many aspects of biomedical industry and practice. The direct link can be found at <http://www.fda.gov/ohrms/dockets/dockets/00d1541/00d1541.htm> and exists under the general heading of “00D-1541: Electronic Signatures: Audit Trails.” This site is the official repository for the administrative proceedings and rule-making documents for the Food and Drug Administration.

The use of EDC in the collection of worldwide healthcare information in clinical trials is predicted to increase significantly over the next few years. Reports that have extensively interviewed the pharmaceutical industry calculate a 2000% increase in the use of technology to collect clinical trial data by 2004. Data can be gathered from healthcare professionals as well as directly from patients in their living rooms, logistically, economically and securely via the public Internet. The value proposition to the pharmaceutical industry is equally dramatic when compared to paper methods, resulting in tens of millions of dollars in cost savings, proven acceleration of the drug development process, and importantly, an elevation in the quality of data collected. Such conditions will also result in a progressive increase in the number of products and companies competing for this explosive global market.

Given these conditions, a very dynamic environment will be quickly created and it is imperative that not only Regulations keep pace with this progress, but also that newer technologies respect methods and processes that have served society well with, albeit less exciting, but well-proven paper models of workflow. We should not regress in process for the sake of “moving forward” with technology. Both conditions must be satisfied for true innovation to be claimed. Education is the strongest bridge in transitioning from the proven to the better.

“The public docket at the FDA serves as an open and objective forum for individuals and companies to share their stances on important issues in healthcare for all to see and learn from,” stated Dr. Jeffrey A. Green, President & CEO of DATATRAK International, Inc. “The docket process is yet another method for our Company to make sure that it stays current with regulatory requirements so that we can best serve our growing worldwide customer base. It is important that proper education be accomplished with all groups that will be associated with the growing use of technology in clinical trials. The use of EDC will increasingly touch regulators, clinicians, FDA Advisory Panels, auditors, investigative staffs



Regulatory Subgroup

at research sites, and even patients themselves. Moving forward with appropriate methodologies will save time, money and will, as best as possible, protect public safety. Just as all drugs in a therapeutic category are not identical in their efficacy or adverse effect profiles, all technology products are not the same. Publication of this Audit Trail Analysis promotes an environment for additional input and the sharing of thoughts to eventually serve as proper guidance for all of us responsible for appropriately advancing the paradigms of clinical research.”

DATATRAK International, Inc. is a worldwide ASP for the EDC industry. The Company provides a suite of software products known as DATATRAK EDC(TM) and related services to the pharmaceutical, biotechnology, and medical device industries. DATATRAK EDC(TM) delivers clinical research data from investigative sites to sponsors faster and more efficiently than traditional manual methods. DATATRAK EDC(TM) can be deployed globally via a distributed platform using laptop computers, in a centralized environment with resident hardware, or in a wireless mode, all utilizing the Internet. DATATRAK EDC(TM) software and its previous versions have successfully supported over 60 international clinical studies involving thousands of clinical research sites and tens of thousands of patients in 31 countries. DATATRAK International Inc.'s product suite has been utilized in the clinical development of 13 separate drugs that have received regulatory approval from either the United States Food and Drug Administration or counterpart regulatory bodies in Europe. DATATRAK International, Inc. has offices located in Cleveland, Ohio and Bonn, Germany. Its common stock is listed on the Nasdaq Stock Market under the symbol "DATA".

Visit the DATATRAK International, Inc. web site at www.datatraknet.com or www.datatraknet.de.

Except for the historical information contained in this press release, the statements made in this release are forward-looking statements. Factors that may cause actual results to differ materially from those in the forward- looking statements include the ability of the Company to absorb corporate overhead and other fixed costs in order to successfully market the DATATRAK EDC(TM) software; the development and fluctuations in the market for electronic data capture technology; continued unreliability of the Internet infrastructure; the degree of the Company's success in obtaining new contracts; the timing of payments from customers and the timing of clinical trial sponsor decisions to conduct new clinical trials or cancel or delay ongoing trials; dependence on key personnel; governmental regulation; the early stage of the Company's EDC business and operations; and general economic conditions. In addition, the Company's success depends on the outcome of various strategic initiatives it has undertaken, all of which are based on assumptions made by the Company concerning trends in the clinical research market and the health care industry.

Contacts: Dr. Jeffrey A. Green, President & CEO; Phone 216-921-6505 x112

Mr. Terry Black, CFO; Phone 216-921-6505 x110

R J Falkner & Company, Investor Relations Council; Phone 800-377-9893