

<u>Signën Clinical Discoveries - LTD</u>	
Affiliate Location: Jeddah, Saudi Arabia Date: 26 February 2009	
Title: Signën Clinical Discoveries_- Data Privacy Policy	
Authorized Signature:	Date: 26 February 2009
Third Party Approval:	Date: 26 February 2009

Abstract

The privacy of any subject who participates in a clinical trial must be protected on both ethical and legal grounds. Data management professionals must be familiar with the privacy issues which apply to their study and ensure that all reasonable and appropriate precautions are taken. This policy discusses the strategies and considerations which the data management professional must understand and follow, including types of personal data in clinical trials, best practice for securing and protecting data (both paper and electronic) from unauthorized access, methods of data collection, and strategies for ensuring that personnel both internal and external (e.g., vendors) follow applicable data privacy standards.

Introduction

As the rapidly changing pace of technology produces new breakthroughs in data storage, linkage, and mining techniques, policies and procedures regarding data privacy must be re-examined. This policy isl define the minimum standards and best practices for ensuring data privacy throughout the data management process.

Data privacy refers to the standards surrounding the protection of personal data. Personal data can be defined as any information that can lead to the identification, either directly or indirectly, of a research subject. Some examples of personal data are patient names, initials, addresses, and genetic code.

The ICH Guideline for Good Clinical Practice (GCP) states: “The confidentiality of records that could identify subjects should be protected, respecting the privacy and confidentiality rules in accordance with applicable regulatory requirement(s).”

Privacy protection afforded to research subjects includes:

- Protocol review and approval by an institutional review board (IRB)
- Right to informed consent
- Right of the subject to withdraw consent

- Right to notice of disclosure
- Confidential collection and submission of data

Although the majority of issues with data privacy rest with site management or clinical-monitoring functions, data management professionals should at a minimum be familiar with basic data-privacy issues and follow principles established by their company to ensure the privacy of research subjects and compliance with GCP.

Throughout the data collection and management process, data management professionals are often exposed to media that includes primary medical and hospital records, genetic data, economic data, adverse drug event reports and several other sources.

It is not practical to have complete anonymity. However, due to concerns for the prevention of scientific fraud and the possible consequences of an intervention or treatment while enrolled in a clinical trial, it is critical that personal information is safeguarded to the greatest extent possible.

Scope

This policy is focusing on the considerations for building and maintaining a platform to maintain a high degree of privacy protection (or security) for research subjects during the data-collection and management procedures. With the complexity of clinical trial strategies, data can be transferred between sites, departments, subsidiaries, and countries.

Since significant regulatory guidance exists on data privacy, all applicable regulations are considered during the creation of this policy to ensure full compliance with regulations governing the jurisdictions in which business is conducted.

Minimum Standards:

- Educate all personnel who directly or indirectly handle personally identifiable data on company procedures and data privacy concepts. Training sessions should include company policy; regulatory agency policy; and applicable local, state, federal, and international law.
- Design data-collection instruments with the minimum subject identifiers needed, including the design of case report forms, clinical and laboratory databases, data transfer specifications, and any other area of data collection that may contain personal information.
- If identified, blind or otherwise address documentation (e.g., CRFs, lab reports) submitted to data management that contains any

additional subject identifiers other than those used to link the documentation to a database record.

- Review and update data management processes regularly to ensure consistency with company privacy policies.

Best Practices

- Develop and maintain an environment that respects the privacy of research subjects. Consider long-term employee education programs that highlight the potential impact of lapses in data privacy, the benefits of applying strict criteria when handling personal information, and the verification that procedures are in compliance with regulations.
- Implement procedures that occur prior to transfer of data to between sites, departments, subsidiaries, and countries to ensure that all considerations about privacy have been considered, addressed, and documented
- Promote internal and external accountability through company policy and regulations governing the use of personal information.
- Collect or use personal data only when required for specific scientific reasons. Ensure that the reasons for use of such data are documented and justified.
- Implement procedures for using data for an alternate or new purpose other than what was originally intended by the informed consent. Ensure that all privacy considerations have been considered, addressed, and documented.
- Enforce a baseline policy of denying access to personal data. Evaluate any request for this information. If the information is determined to be required for specific scientific reasons, ensure that all considerations about privacy have been considered, addressed, and documented.
- Put special procedures in place to store, access, and report on extremely sensitive data, such as any type of genetic information.
- Make compliance with data privacy regulations a central focus of audits and a contract contingency when using external service providers.
- Maintain proper physical and electronic security measures. Data should be stored in protective environments relevant to the type of media being stored. Paper case report forms should be stored in an environment with regulated access. Proper precautions, such as password authentication and firewall security, should be taken to prevent external access to data.
- Address any data submitted to data management that appears to have been collected without the obtaining of consent or authorization from the research subject.

Data Collection

To ensure proper assignment of data in a clinical database, data collection instruments should be designed with the need for the minimum research subject identifiers. The use of these identifiers should be taken into consideration not only in case report form design, but also in scenarios in which the processing, transfer, reporting, or analysis of data will be completed. These scenarios include the design of clinical databases, laboratory databases, and data-transfer specifications. In general, a random subject number and gender can be used to resolve any discrepancies that might arise from transcription errors.

Although it is the responsibility of the investigator to ensure that subjects have been given a proper informed consent, it may be beneficial to create a case report form module that contains the following question: “Did the subject read, understand and sign the informed consent?” This question allows data management to process data into the clinical database with confidence that proper consent was acquired.

If source documents are to be collected (i.e., radiology, MRI, or ECG reports), the sites should be instructed that all documentation should be stripped of personal identifiers and that appropriate subject identifiers should be assigned prior to submission to data management. If that direction is not followed, data management should follow up with the appropriate internal or external clinical site management and ensure that follow-up and further direction is recommended for specific site violators.

Recent scientific advances in the area of genetics have now made it possible to store the ultimate identifier, subject DNA. Utmost care should be taken to isolate and protect this data. Strict standards should be adopted, including completely independent data servers and storage facilities, separate groups to manage genomic data, and specific standard operating procedures dedicated to the processing and use of this data.

Ensure that any external vendors subscribe to standards that meet or surpass internal standards. For example, lab reports generated from central labs should not contain any subject-specific information. This information should be built into data-transfer and reporting specifications. As an overall strategy, ensure your company is performing external audits of vendors that include investigations into their compliance with regulations on the protection of personal data.

Physical and Electronic Data Security

All paper or electronic data should be safeguarded with high standards. Standard operating procedures should be reviewed on a regular basis to ensure the latest data-protection standards are being implemented.

Policy Definition and Training

Corporate policy definition and training should be based on relevant company policy; regulatory agency policy; and applicable local, state, federal, and international law. The policy training sessions should address the implementation and maintenance of standards and potential harm to subjects that may occur when basic principals are not followed.

===== End of Document =====