Data Privacy

April 2009

Abstract

The privacy of any subject who participates in a clinical study must be protected for ethical and legal reasons. Clinical data management professionals must be familiar with privacy laws that exist for the regions in which clinical studies are occurring and ensure all reasonable and appropriate precautions are taken. This chapter discusses strategies and considerations that data managers must understand and follow, including the varying types of personal data in clinical studies, best practices for securing and protecting data (both paper and electronic), methods of data collection, and strategies for ensuring that personnel, both internal and external (e.g., vendors), follow applicable data privacy standards.

Introduction

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

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)."[1]

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 and have no further data collected

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

Although the majority of data privacy responsibilities rest with site management or clinical monitoring, data management professionals should be familiar with basic data privacy issues and follow regulatory and organizational guidelines to ensure the privacy of research subjects.

Having complete anonymity may not always be practical for the design of a study, however, personal information should always be safeguarded to the greatest extent possible.

Scope

This chapter focuses on considerations needed to maintain a high degree of privacy protection (or security) for research subjects during data collection and management. Since significant regulatory guidance exists on data privacy, all applicable regulations should be considered in the creation of company policy or standard operating procedures (SOPs) to ensure full compliance with regulations governing the jurisdictions in which business is conducted. References for various regulatory documents can be found in the Further Reading section of this chapter.

Many of the tasks described in this chapter may be joint responsibilities between different groups, just as there may be many different groups involved in the implementation of various tasks. However, clinical data managers need to be conscious of whether or not these tasks have in fact been performed in a satisfactory manner.

Minimum Standards

- Ensure all personnel (including vendors) who directly or indirectly handle identifiable personal data are properly trained on data privacy issues. Training sessions should cover data privacy concepts; company policy; regulatory agency policy and applicable local, state, federal, and international laws.
- Design data-collection instruments with the minimum subject identifiers needed, including the design of case report forms (CRFs), clinical and

laboratory databases, data transfer specifications, and any other area of data collection that may contain personal information.

- Ensure personal data is not identifiable, other than subject identifiers used to link documentation to a database record, from documentation (e.g., CRFs, lab reports, images associated with the clinical study) submitted to data management.

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

Best Practices

- Develop and maintain an environment that respects the privacy of research subjects. Consider employee education programs that highlight the potential impact of lapses in data privacy, the benefits of applying strict criteria when handling personal information, and verification that procedures are in compliance with regulations.

- Implement procedures prior to data transfer between sites, departments, subsidiaries, and countries to ensure all privacy considerations have been considered, addressed, and documented.

- Promote internal and external accountability through company policies and regulations governing the use of personal information.

- Implement procedures for using data for an alternate or new purpose other than what was originally intended by the informed consent. Ensure 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 information is determined to be required for specific scientific reasons, ensure all privacy considerations have been considered, addressed, and documented.

- Put stringent procedures in place to securely transfer, store, access, and report on extremely sensitive data (e.g., genetic information).

- Work with those responsible for quality assurance to ensure compliance with data privacy regulations. This assurance of regulatory compliance should be 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 CRFs should be stored in an environment with regulated access. Proper precautions should be taken to prevent external access to electronic data, such as password authentication and firewall security.

Importance of Data Privacy

Revealing a subject's personal medical information could potentially lead to embarrassment, denial of insurance coverage, or discrimination in the workplace. For these and other reasons, most countries have passed stringent laws that mandate the protection of research subjects' privacy.

Every organization with access to subjects' personal data should have SOPs addressing data privacy. At a minimum these SOPs should comply with all regulations of the study locale, although many organizations put SOPs in place that are stricter than required by local regulations.

All personnel with access to personal data must be adequately educated in data privacy related SOPs. The reasons for data privacy, what constitutes personal data, and how to handle various situations that may arise in the course of the study should be explained.

The data manager's role has a narrower focus than an investigator site in regards to data privacy. Nonetheless, the data manager needs to ensure data privacy is maintained throughout all aspects of data management.

Legislation and Regulatory Guidance

Legislation and guidance documents from the EU and US have a greater impact on clinical research than laws in other countries, because the EU and US are involved with a higher volume of clinical research. In Europe, EU Data Protection Directive 95/46/EC, which became mandatory in October 1998, covers privacy of all types of personal data including data from clinical studies.[2] Directive 2001/20/EC subsequently became mandatory in May 2004

and expanded upon the previous directive in relation to data privacy and informed consent in clinical studies.[3] One of the stipulations of these directives is that members of the EU are not allowed to transfer personal data to countries that the EU Commission has determined lack adequate subject privacy standards. Countries that are found to have adequate privacy standards are given an "adequacy determination" by the EU Commission. In regards to the US, the EU has agreed to give *individual* US companies an adequacy determination if they meet the privacy standards of the EU.[4] As a result, many US companies have adopted the stricter privacy requirements of the EU.

The processes for US companies to acquire an adequacy determination are known as Safe Harbor Principles, and were developed by the US Department of Commerce in collaboration with the EU. Once a company receives an adequacy determination through adherence to these principles, they must recertify every 12 months. According to these principles, companies must provide the following:

- Notice—Subjects must be informed of how their data will be collected and used.
- Choice—Subjects must be able to opt out of collection of their data and its transfer to third parties.
- Data transfers—Any transfers of data to third parties must only be to other organizations that have rigorous data-protection policies.
- Security—All reasonable efforts must be made to prevent the loss of any data collected.
- Data integrity—Data must be reliable and relevant to the purpose for which it was collected.
- Access—Subjects must be able to access information about them that is collected, and have an opportunity to have this data corrected or deleted if necessary.
- Enforcement—A mechanism must be in place to effectively and consistently enforce these rules.

It is recognized that laws dealing with medical data privacy in the US are more fragmented than those of the EU. One example of this fragmentation is the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which went into effect in April 2003.[5] Although HIPAA covers a wide range of organizations possessing health data, research recruitment organizations, clinical research organizations and pharmaceutical companies fall outside HIPAA's purview.[4] Other US privacy laws include Section 5 of the Federal Trade Commission Act (15 United States Code § 45(a)(1)), the Gramm-Leach Bliley Act (15 United States Code, Subchapter 1, § 6801–6809), several parts of Code of Federal Regulations Titles 21 and 45, and numerous state laws regarding data privacy. *ICH Guideline for Good Clinical Practice* and various FDA guidance documents give additional advice and directives for privacy issues in clinical studies, but are not legally binding documents.

What Constitutes Private or Personal Information?

According to EU Directive 95/46/EC, personal data "shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[2]

Similarly, 45 CFR Section 164.501 (HIPAA) defines individually identifiable health information as "…information that is a subset of health information, including demographic information collected from an individual and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual."[5]

Data Privacy Focus Areas

Clinical data managers should make every effort to ensure access to data is restricted to qualified and approved personnel. In particular, the following areas should be examined to ensure appropriate data privacy is maintained.

Vendors with Access to Data

Different standards may need to be employed for vendors who only have access to vendor-specific data versus those who have access to the study database and all subject-associated data. For those vendors having access to the database, the data manager should ensure that the vendors subscribe to standards that meet or surpass internal standards. As an overall strategy, ensure your company is performing external audits of vendors that include investigations into their compliance with regulations concerning the protection of personal data.

Lab Data

Reports generated from all types of labs should not contain any subject-specific information. This information should be built into data-transfer and reporting specifications.

If source documents are to be collected (e.g., radiology, MRI, or ECG reports), the sites should be instructed that all documentation should be stripped of personal identifiers, and 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 to ensure that follow-up and further direction is recommended for specific site violators.

Central Committees

Reports to and meetings with various committees may necessitate presentation of some study data. Different types of committees may require different data points and data sources, according to the committee's function. A committee may require reports based on the database, data from the database, original source data or copies of source data. In all cases, personal subject identifiers should be removed prior to presentation of data to the committee, and in some

cases, study identifiers may need to be added. The parties responsible for anonymity of the data may vary depending on the type and source of the data. Someone independent of the study may be utilized when necessary to ensure data anonymity, such as a liaison between the company and the committee.

Data transfers

Prior to any data transfer, a data transfer specification document should be produced to identify the secure method of transfer and fields to be transferred, including the data keys and structure. Before any data is transferred, the transfer process should be thoroughly tested to ensure no extraneous information is transferred that could jeopardize data privacy. Once the planned data transfer is performed, the transfer should be reviewed to ensure all transferred data matches the database.

Computer and network security

Computer and network security are typically developed and maintained by an organization's information technology personnel. However, data managers do have a responsibility to ensure that the systems are used appropriately and responsibly. Any lapses in computer or network security may jeopardize the integrity of the database, and therefore, data privacy.

Appropriate Redaction of Personal Data

Redaction is the act of obscuring or removing text from a document before releasing the document to other personnel or departments. An example of clinical data needing to be redacted could include a situation where a comments field was completed with personal identifiers. If for example a comments field had the text "Mr. Jones showed improvements," the data manager should obscure or remove "Mr. Jones" from this text. Organizations should have SOPs to determine when redaction of personal data is needed. This should preferably be performed by the site or monitor, but if not handled at the site, data managers should be mindful of when redaction of personal data is required as well as knowledgeable on the process.

Data Collection

To ensure proper assignment of data into a clinical database, data collection instruments should be designed with some type of research subject identifiers. The use of these identifiers should be taken into consideration not only in CRF 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 can be used to resolve any discrepancies that might arise from transcription errors.

Recent scientific advances in genetics have made it possible to capture the ultimate identifier, subject DNA. Utmost care should be taken to protect this data. Strict standards should be adopted, including storage in completely independent data servers and physical locations, independent resources to manage genomic data, and specific SOPs dedicated to the processing and use of this data.

Variance Between Data Collection Methods

Different data collection methodologies may necessitate different considerations to maintain privacy of data. The following are common considerations for different collection methodologies.

- Paper-based studies—Follow organization SOPs for appropriate redaction of personal identifiers as well as appropriate study procedures for handling, transfer and storage of documents containing privacy data.
- EDC studies—Follow organization SOPs to ensure appropriate network security, including password security and automatic user logout after a determined period of time.
- ePRO—Follow organization SOPs to ensure appropriate network security, as well as training of subjects on use of devices and protection of data by use of assigned passwords and user identification or pin numbers.

International Studies and Data Privacy

International studies should adhere to the most restrictive regulations of the countries involved. However, ensuring data privacy also needs to be balanced with the need for collecting all data pertinent to the study. Some questions to ask in this regard may include:

- Is the data really needed?
- Does collection of needed data compromise privacy?
- Is collection of the data acceptable in all countries with study sites?

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. Policy training sessions should address the implementation and maintenance of standards and potential harm to subjects that may occur when basic principles are not followed.

Potential Future Concerns for Data Privacy

Electronic health records and their potential integration with EDC systems are expected to garner more attention in the future. Although there is currently no mandate to use electronic health records, the topic has been discussed frequently not only by those involved with health care or clinical studies, but also within political circles. If health records do become exclusively electronic, new safeguards will be needed to ensure privacy of these records.

Recommended Standard Operating Procedures

- Organization Procedures for Data Privacy Protection
- Vendor Management

References

1. International Conference on Harmonisation. *Harmonised Tripartite Guideline for Good Clinical Practice*. 2nd ed. London: Brookwood Medical Publications; 1996.

2. European Parliament and Council of Europe. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Strasbourg, France: European Parliament and Council of Europe; 1995. Available at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm. Accessed November 10, 2008.

3. European Parliament and Council of Europe. Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use. Strasbourg, France: European Parliament and Council of Europe; 2001. Available at: http://ec.europa.eu/enterprise/pharmaceuticals/eudralex/vol1_en.htm. Accessed November 10, 2008.

4. Antokol J. Protecting Personal Data in Global Clinical Research. *The Monitor*.2008:22;57–60.

5. Code of Federal Regulations, Title 45, Part 164.501, Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Washington DC. US Government Printing Office; 2002. Available at: http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr164_02.html. Accessed November 10, 2008.

Further Reading

Love CB, Thomson EJ, Royal CD. Current Bibliographies in Medicine 99-3: Ethical issues in research involving human participants Web page. Available

from: http://www.nlm.nih.gov/archive//20061214/pubs/cbm/hum_exp.html. Accessed November 10, 2008.

United States of America

US Department of Commerce. Safe harbor documents Web page. Available at: http://www.export.gov/safeharbor/SH_Documents.asp. Accessed on November 10, 2008.

US Department of Health and Human Services. *Health Insurance Portability and Accountability Act of 1996*, (HIPAA) Public Law 104-191, as amended, 42 United States Code 1320-d. Washington, DC: US Government Printing Office; 1996. Available at: http://aspe.hhs.gov/admnsimp/pvcrec0.htm. Accessed on November 10, 2008.

US Department of Heath and Human Services Data Council. Office of Data Policy Web page. Available at: http://aspe.hhs.gov/datacncl/. Accessed November 10, 2008.

US Department of Health and Human Services. *Code of Federal Regulations*, Title 45, Volume 1, Parts 160 and 164. Washington, DC: US Government Printing Office; 1998.

US Department of Justice. *Federal Privacy Act*, 1974. PL 93-579,5 USC 552a, as amended. Washington, DC: US Government Printing Office; 1974. Available at: http://www.usdoj.gov/oip/privstat.htm. Accessed November 10, 2008.

European Union

The European Group on Ethics in Science and New Technologies. *Opinion No. 13: Ethical Issues of Healthcare in the Information Society*. Brussels, Belgium: The European Commission; 1999. Available at: http://europa.eu.int/comm/european_group_ethics/docs/avis13_en.pdf. Accessed November 10, 2008.

European Parliament and Council of Europe. *Directive 95/46/EC of the European Parliament and of the Council 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data*. Strasbourg, France: European Parliament and Council

of Europe; 1995. Available at: http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0045.html. Accessed November 10, 2008.

Australia

Attorney-General's Department. *Privacy Act 1988. Act No. 119 of 1988, as amended.* Canberra, Australia: Office of Legislative Drafting and Publishing; 2006. Available at: http://www.privacy.gov.au/publications/Privacy88_100107.pdf. Accessed November 10, 2008.

National Health and Medical Research Council. *National Statement on Ethical Conduct in Research Involving Humans.* Canberra, Australia: Commonwealth of Australia; 1999.

Canada

Kosseim P, ed. *A Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research*. Ottawa, Canada: Public Works and Government Services; 2005. Available at: http://www.cihr-irsc.gc.ca/e/documents/ethics_privacy_compendium_june2005_e.pdf. Accessed on November 10, 2008.

Office of the Privacy Commissioner of Canada. *Personal Information Protection and Electronic Documents Act. S.C. 2000. c.5.* Ottawa, Canada: Office of the Privacy Commissioner of Canada; 2000. Available at: http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp. Accessed November 10, 2008.

Chapter Revision History

Publication Date	**Comments**
September 2003	Initial publication.
May 2007	Revised for style, grammar, and clarity. Substance of chapter content unchanged.
April 2009	Revised for content, style, grammar, and clarity.