CHAPTER 4

PRIVACY, CONFIDENTIALITY, AND PROTECTION OF PERSONAL INFORMATION

Key Points:

- **Protecting the privacy of human research subjects and confidentiality of information acquired about them in the course of research is particularly important in worker studies because of the possible personal or economic damage to the worker that can result from the release of confidential data.**

- **Proper management of study data must consider the: (1) use of data by others, (2) sharing of data, (3) use of personal identifiers, (4) use of pre-existing data, (5) appropriate dissemination of data and results, and (6) worker's rights regarding personal data and results. The data management plan must be part of the research plan approved by the IRB and should be disclosed when obtaining informed consent.**

- **The collection and use of genetic information, human tissues, and biological samples exposes, subjects to individual risks from the acquisition and use of confidential data about them and their families. These risks create an additional set of complex ethical concerns that require the awareness of all stakeholders.**

Expectations of Privacy and Confidentiality

Protection of subjects' privacy—and the confidentiality of information about them—is essential for the successful conduct of worker studies. How the research team handles confidential information about workers will determine if a relationship of trust is to be established and maintained.

> **Confidentiality:** The treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others without permission or in ways that are inconsistent with the understanding of the original disclosure (in informed consent documents).

Workers should have a reasonable expectation that personal information will be disclosed to others only with their permission or in ways that are consistent with their understanding of the original disclosure, the informed consent documents, or in compliance with the law.

Privacy Protections

Various state and federal laws, as well as the requirements of IRBs, seek to protect the confidentiality of individually identifiable research information. Regardless of the good intention of others for the protection of their privacy, **absolute protection of data cannot be guaranteed.** Although penalties exist in both federal and state law for a breach of confidentiality, breaches of confidentiality may be inadvertent (accidental), deliberate (knowingly done) or compelled (by regulation or law).

> **Privacy:** An individual's control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.

Breaches of confidentiality may have serious consequences for the study participant. Fear of discrimination, misuse of genetic information, loss of health insurance, or loss of privacy—all of which may result from breaches of confidentiality—are serious issues that must be addressed in a study design. The proper management of study data, including clearly defined and strictly followed procedures to protect the confidentiality of study participants, can significantly reduce the possibility of such breaches and must be part of every study design.

Workers' concerns about access to collected research data may cause them to choose not to participate in a study. A related concern about the confidentiality of occupational medical records may lead some workers to choose not to use their workplace health services. For example, a worker might decide not to take part in medical screening, fearing that the results could become known and limit his or her employment, economic advancement, or insurability.

> Researchers, employers, and other stakeholders involved in worker studies should consider access to records as a special obligation to workers as research subjects.

Although participants in a worker study should be aware that future researchers, federal agencies, insurance companies, employers, and others might obtain legal access to the

data, it is also true that researchers can protect the confidentiality of data gathered about a subject. For example, researchers can eliminate personal identifiers by using codes during the study and purging identifiers as soon as possible.

When personal tissues or bodily samples, such as blood or urine, are obtained from workers, the workers must be assured, during the informed consent process, of the plans for present and future use, labeling, storage, ultimate disposition, and access restrictions to the materials and data. Federally funded research using human tissue that is not exempt from human subjects regulations must be reviewed by an IRB. Examples of research that may be **exempt** from informed consent or IRB review include:

- Research performed on tissue or data from deceased subjects.

- Collection or study of existing data documents, records, and pathologic or diagnostic specimens, if these sources are publicly available or if the data are recorded by an investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects. The specimens must have been collected before the research study in which they are to be used was conceived and cannot contain any direct or indirect identifiers that could allow the investigator or collaborators to link the specimens to subjects' identities.

Exemption from IRBs not Always Applicable

The exemption from IRB review does not apply when the research requires the collection of follow-up data on subjects from whom the specimens were obtained such as is customarily the case in worker studies or, more generally, when samples can be linked to individual identities. Also, institutional policy may require review of research that is otherwise exempt.

Access to Research Data and Personal Records

The conditions under which an employer or another party may have access to personal information gathered for a study or to analyze results must be clearly explained to the study participants. Federal and state laws vary in the privacy protection given these kinds of information. For example, the Privacy Act of 1974 protects personal information held in federal agency records from unauthorized disclosure. Only the subject of a protected record has access to that record, with certain exceptions such as the "routine use" of the data (defined below).

Contractor Records

Not all records at federal agency sites are federal records. Some records belong to the contractors and may not be subject to laws governing the management of and access to federal records. Contractors' records are governed by the specific terms of their agency contracts. In particular, access to these records is governed by the terms of those contracts and by the law, including the agency's Freedom of Information Act regulations on contractor records (10 CFR 1004.3[e]).

To carry out studies, researchers may require access to records and data owned by agency contractors. Contractor-owned records needed for health research that contain personal identifiers are made available under the access authority of the ownership-of-records clause of the governing contract, and access is subject to the Privacy Act.

The IRB review should ensure that the research protocol protects the confidentiality of contractor-owned records made available in worker health studies. Many states impose additional, independent requirements to protect the confidentiality of records used for research.

Federal Records

The **Privacy Act of 1974** establishes safeguards for the protection of some of the records the government collects and maintains on individuals. It specifically mandates that the government prevent disclosure of information in agency Privacy Act "systems of records" without the consent of the individual to whom they pertain except under certain conditions. These conditions include situations where disclosure would be required under the Freedom of Information Act and in other situations including where disclosure would be for a "routine use."

A Privacy Act **system of records** is a group of any records about an individual under the control of a federal agency from which the information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Many federal contracts have an **ownership of records** clause that specifies which records are considered government-owned even though they are in the custody of a contractor. This "ownership" clause extends Privacy Act protection to these records, however, these records, including records containing personal identifiers may be made available to health researchers under "routine use" provisions.

A Privacy Act **routine use** is a use of such record for a purpose that is compatible with the purpose for which it was collected and maintained. The federal agency must publish in the Federal Register notices of all agency Privacy Act Systems of Records, including in each notice a list of routine uses for that system.

The possibility of "routine use" of data by others should be described in the study's scope of work. There should be a clear statement that the data cannot be shared with others without authorization and IRB approval. Anyone seeking permission for further access to the data must obtain permission from the office that originally authorized its use in the study. Subjects should be advised of the possibility of these "routine uses" as part of the informed consent process.

The Privacy Act also establishes safeguards against an invasion of privacy through the misuse of records by federal agencies. Specifically, it mandates that the government:

- Inform people why the information is being collected and how it will be used.
- Publish a notice in the Federal Register of new or revised systems of records on individuals.
- Publish a notice in the Federal Register before conducting computer matching programs.
- Ensure that information is accurate, complete, relevant, and up-to-date for agency purposes and before disclosure.
- Allow U.S. citizens and legal aliens access to records about themselves and to find out disclosures of their records to other agencies or persons.
- Provide U.S. citizens and legal aliens the opportunity to correct inaccuracies in their records.
- Prevent disclosure of privacy information without the consent of the individual except under certain lawful conditions.

The Privacy Act governs access to data only for: (1) researchers who are federal employees or (2) contractors who must sign an agreement documenting data security procedures and confirming that they will comply with the privacy and confidentiality requirements of the Privacy Act.[1] Individual researchers funded by federal agency grants are ***not*** bound by the Privacy Act, but they may have to sign an agreement with the agency to protect the confidentiality of the records to which they are given access.

In contrast to the Privacy Act, the **Freedom of Information Act**, 5 U.S.C. 552, generally provides that any person has a right of access to federal agency records. However, one is not entitled to such records to the extent that such records, or portions thereof, are protected from disclosure by one or more of the nine exemptions or by one of the three special law enforcement record exclusions found in the statute. One of those exemptions is especially important for studies that involve the worker community. This is Exemption 6 that authorizes an agency to withhold "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," (5 U.S.C. 552[b][6]).

A data management plan should be part of the overall research plan that is reviewed by the IRB. Protection of privacy and confidentiality of records may be achieved in any one or a combination of the following:

- The use of codes to replace individual identifiers.
- Purging identifiers when no longer needed.
- Aggregating data in reports and publications, thereby not presenting individual records.
- Obtaining written consent when information is shared or used in a manner not covered in the informed consent.
- Information obtained or recorded should be limited to only that information needed for the research effort.

Note: Subjects should be advised that absolute confidentiality may not be possible, and that disclosure may be compelled by local, state, or federal laws.

[1] For additional guidance on access to records for health studies, see the DOE *Access Handbook* referenced in the bibliography.

Clearly, employees, contractors, and researchers must adhere to these rules of conduct to protect individual personal information from the possibility of unwarranted disclosure or access by unauthorized persons.

Congress, state legislatures, and government agencies continue to struggle with legislation to control access to, and the use of, private personal and medical information. New or revised legislation could further restrict or limit the use of personal data and human tissue samples for research or for other uses.

Record of Disclosure

Where research or medical records are protected by the Privacy Act, federal employees must keep an accurate record of the date, nature, and purpose of most disclosures of a record to any person or to another agency. If authorized by law, disclosure of these records may be made for civil or criminal law enforcement activities. The worker may request and receive the name and address of the agency or person to whom his or her information was disclosed in most cases.

Certificate of Confidentiality is a certificate, issued under the authority of the Public Health Act Section 301(d), 42 U.S.C. 241(d), which will "protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of research the names or other identifying characteristics of such individuals."

Certificate of Confidentiality

Under federal law (and some state laws) researchers can seek an advance "Certificate of Confidentiality" where unwarranted release of highly sensitive information could harm the subject. A certificate of confidentiality, issued by the Assistant Secretary for Health or by NIH, on a project-by-project basis, adds protection for subjects by providing limits on the compelled disclosure of identifying information.

The HHS policy includes as "sensitive" research, information that could, if released, damage the individual's "financial standing, employability, or reputation within the community" or the disclosure of which could lead to "social stigmatization or discrimination." Examples of "sensitive" research include mental illness, sex research, AIDS and HIV status, and illegal drug use.

Holders of a Certificate of Confidentiality may not be compelled in federal, state, criminal, legislative, or other proceedings to identify individual research subjects. Such added protection may encourage candidate subjects to participate in these studies.

Certificates of Confidentiality may have limited value in that they give researchers the right to avoid compelled disclosure in a legal proceeding, but they give no rights to the research subject to *insist* on their use. Additionally, they provide no remedy or recourse in the event of disclosure in instances of violation.

Secondary Analysis and Data Sharing

The secondary analysis of data, which includes data sharing with third-party researchers or other outside organizations, can be of concern in protecting the worker's privacy. The study plan must consider the ultimate use of data with and without identifiers, the consequences of destroying individual codes or identifiers, the access of the subject's personal physician to the data, and the problem of keeping research data separate from medical records.

Inclusion of research results in medical records, which are available for review under a routine use of data option, may put the worker's insurability or financial status at risk. Under the Privacy Act, research results, if previously specified to be a part of the medical records, will become part of those records regardless of whether this is authorized by the research subject or not.

Furthermore, the practice of conducting or permitting several studies (multiple studies) with the same or similar goals and using the same worker population should be evaluated to reduce duplication. Therefore, local IRBs must review ***all*** worker-studies applicable to the worker population for which they are responsible. Not only do the studies become intrusive but also, as stated earlier, additional access to worker data by multiple parties increases the risk of loss of confidentiality, and raises fears and confusion among potential subjects.

When multiple studies on the same worker population are approved, the worker community should be adequately informed of the nature and need for such studies well in advance. Otherwise such studies may create the perception that they are being performed because something is medically "wrong" with the individual, or that some improper activity is being undertaken that must be hidden from public view.

Dissemination of Data and Results

Ideally, research results should be published after an independent scientific peer review to avoid the risk of disseminating spurious results. Furthermore, the disclosure of information that may have been discovered as a result of research may result in inadvertent discrimination against identifiable populations or worker communities.

Generally, while it may be unethical ***not*** to publish research results, care must be taken to assure that their publication does not pose a potential, unintended risk to a study population that is greater than the realized benefit of publishing the results. In such cases, the research team should publish or disseminate the results after consultation with stakeholders and peer reviewers to assure that a balance is achieved between the need to publish results and the possibility of group discrimination or harm. When publishing results, researchers should choose report language carefully and avoid the use of group identifiers in order to mitigate any harmful impacts to a community.

Communication with Study Participants

The study methodology and research plan should include a system for transmitting study results, study conclusions, and their implications to the subjects and other interested parties in a timely manner. Consideration should be given to those study participants who may not wish to be informed of the research results. Employers, employees, and unions should be informed of all research questions, the study methods to be used, and any limitations in analysis and interpretations.

Feedback on overall findings also is important to the worker group. This is especially true when medical tests are involved, even if the researchers have not analyzed the data to the point at which they can give the individual feedback. Group results should be provided in readily understandable terms.

> The investigators should clearly indicate where the meaning of a test or result is not known or is inconclusive.

Timely interim reports and feedback are important, are encouraged, and should be disseminated to workers via meetings, handouts, and notice-boards. Any concerns of employers, unions, or individuals need to be fully and frankly discussed and resolved.

Individuals participating in the study should also receive timely, understandable information about their personal results ***if*** they choose to receive it. The informed consent process should apprise participants of their right ***not*** to be told their personal results, or even to have it known that they participated in the study.

In most cases individuals have the right to see their own study or monitoring results and should have ready access to these data. Individuals also have the right to choose *not* to see, or *not* to be informed of, their results. This aspect of the worker's right to choose should be stated in the informed consent documents. An exception might be when experimental assays are being tested and the resulting data are not reliable or clinically validated, and then not providing individuals their results may be the only ethical or legal option.

When applicable, research subjects should also be given the option of having their results sent to their personal physician or other advisor. When an individual's results indicate a significant abnormality, that person should be professionally counseled about the implications of the results and a written explanation and interpretation provided to his or her personal physician. The timing of such counseling needs to be considered. In some cases, counseling may be desirable before results are available as well as before the individual is asked to make other decisions regarding testing or test results.

Study Reports and Publications

It should be noted that the use and distribution of study conclusions and recommendations in the worker community should be anticipated and included in the initial planning of the study and that the IRB(s) must approve the plan.

The peer-reviewed findings and conclusions drawn by worker studies are found in reports and publications of study results and may include recommendations. It is important that the research plan address:

- Plans to document study results.
- What will be done with the information.
- How the stakeholders' knowledge of the results will affect the workers.
- What recourse workers have regarding their reactions to the publication of results (to be discussed during the informed consent process).
- Possible future uses of the data and/or collected or archived biological samples.