NCI/Office of Communications and Public Liaison

APPENDIX 7

CONFIDENTIALITY OF COMMUNICATIONS POLICY

Confidentiality of Communications

Confidentiality

Confidentiality is a value that maintains respect for the privacy of those who use a variety of medically related services. The promise of confidentiality permits a relationship of trust between those being served and those providing service.

Individuals seeking cancer information frequently entrust detailed personal information to National Cancer Institute (NCI) Contact Center (CC) staff so that information can be tailored to their specific needs. CC staff will respect the privacy of all people who contact the Center and are required to sign confidentiality agreements.

Confidentiality extends to the following:

- Identities of patients who are the subject of CC services and communication.
- Identities of physicians who are mentioned in CC services and communication.
- Identities of all other clients who use CC services.

Confidentiality requirements extend to all CC staff, including CC program staff at NCI. If it is necessary to share client information with NCI to provide quality service or with researchers for studies to which clients have consented, it is not considered a breach of confidentiality.

Anonymity

Although confidentiality protects client information, CC staff also respect the wishes of clients who want to remain anonymous. Staff provide all services possible to meet the needs of clients while respecting client anonymity.

Destruction of Identifying Information

Personally identifiable information will be destroyed or de-identified per retention record policies. Exceptions include: Contacts used for quality assurance and training purposes, callbacks, and research studies for which clients have given informed consent. Once service is completed, including any follow-up calls or contacts, identifying information of CC clients is destroyed. CC systems automatically purge identifying information on a set schedule. If information is kept by the CC to complete follow-up calls or contacts, these records are destroyed following completion of the inquiries.

The CC keeps client contact information for longer periods only with the informed consent of the client. This is done to continue providing requested assistance: e.g., to call clients back when an inquiry requires additional research, to conduct approved health communications research projects, or to conduct Office of Management and Budget-authorized data collection for evaluation purposes.

Research Activities

The conduct of research studies within the CC may require the collection and storage of identifying information. Data are collected after obtaining required consent based on the parameters of the research project and in accordance with requirements of Institutional Review Boards (IRB) and NCI. CC clients who participate in research studies must have confidence that data obtained will not be used for other than the stated research purposes or be stored in a way that would compromise confidentiality. The CC does not share research data with those who are not parties to the studies. The timeframe for keeping research data is determined by the scope and purpose of individual research studies.

See Policy 5 *Data Collection in the NCI Contact Center*, and the Information Specialist Training Program Module 6: *Coding and Documentation* for more information.

Legitimate Exceptions to Confidentiality

In some instances, situations arise that supersede a promise of client confidentiality. These situations may include individuals who are a danger to themselves or others or individuals who indicate that they are victims of abuse or individuals who report involvement in or knowledge of a criminal activity.

For phone interactions, CC staff should obtain immediate assistance from a Supervisor and report suspected abusive behavior or threats of to the appropriate counseling, medical and/or emergency personnel.

For online interactions *(LiveHelp and Social Media)*, CC staff should obtain immediate assistance from a Supervisor and report suspected threats of or criminal activity to CCPIB staff. The incidents will be reported to the CyberCrimes Unit of the FBI.