INVENTORY OF
Best Practices Assurance of Confidentiality and Security

Name of Organization: _____

Date: _____

Effectively protecting the confidentiality of individually identifiable data requires uniform and comprehensive practices. Please indicate whether _____ (*firm name or registry)* meets the following best practices guidelines for security and data confidentiality.

General Confidentiality Practices

YES	*NO*	
❍	❍	Employees sign confidentiality agreements.
❍	❍	Confidentiality agreements with staff are signed on a routine basis at a _____ *(month)* interval.
❍	❍	The security practices of the organization have been audited with no material findings.
❍	❍	If material findings were noted, they have been corrected.
❍	❍	Written and explicit institutional policies and procedures are in place to deal with breaches of confidentiality.
❍	❍	Methods are proactive and in place to monitor and detect the adherence to confidentiality protection procedures.
❍	❍	Data submissions are fully protected against legal discovery, including subpoena and freedom of information inquiries.
❍	❍	Organizational or institutional penalties for misuse of confidential data and breach of confidentiality by staff exist, are available in writing, and are enforced.
❍	❍	Access to data files are restricted to specific project staff and access by non-project staff is not permitted.
❍	❍	An individual is formally designated to assure compliance with established institutional standards.
❍	❍	Specific sanctions for confidentiality violation can be imposed that include employee disciplinary action and any of the following: remedial training in confidentiality, loss of certification of competency in confidentiality, prohibition from future work with confidential data at the institution, discharge.

Education

_____ *(Firm or registry)* can assure _____ *(Registry)* that it:

YES	*NO*	
❍	❍	Has developed and implemented education programs regarding confidentiality that includes information about the lack of security inherent in faxing, e-mailing, and other electronic data transfer; reminders about not using names or other personal identifiers in conversations in public

areas such as open labs, elevators, or hallways; and reminders to employees of their special duty to maintain confidentiality when research involves individuals they know personally.

❍ ❍ Formally credentials staff who have received confidentiality training.

❍ ❍ Conducts a routine evaluation of skill and performance with regard to protection of confidentiality an identifies re-training needs based on performance.

❍ ❍ Routine evaluation of employees' skill and performance is conducted.

❍ ❍ Re-training needs are based on performance indicators, either for individuals or groups.

Electronic Security

_____ *(Firm or Registry)* has the following *technical practices* in place:

❍ ❍ Authentication of users by means of passwords or digital ID.

❍ ❍ Access control by means of role-based authentication/access, locked server room, and an internal firewall.

❍ ❍ An audit trail that documents who, when, and for what purpose data (including paper) was accessed.

❍ ❍ A disaster prevention and recovery plan including adequate fire and entry alarms where data are stored; a fireproof file space for paper, routine backups of electronic data at intervals appropriate for the rate of data accrual; and offsite storage of backups (e.g., a safe deposit box).

❍ ❍ External firewalls in places to prevent remote access by unauthorized users.

❍ ❍ Virus checking is routine as are updates to the data files and engines to provide maximum protection of data files.

❍ ❍ System assessment including diagnostics runs and external audits conducted regularly to insure the integrity of the system.

❍ ❍ Data that are sent and received in conjunction with _____ *(Registry)* activities are electronically encrypted.

❍ ❍ A data retention schedule is defined which includes a notation of the date when files are destroyed.

❍ ❍ Data file owners are notified when their file is destroyed.

The *transfer of data* is accompanied by:

❍ ❍ A data-transfer agreement incorporating confidentiality standards to ensure data security at the recipient site and set standards for the data use at the recipient site.

❍ ❍ A paste (electronic) or stamp (paper) on all records containing identifiable data as a reminder of the need for special handling.

❍ ❍ Telecommuting and the use of home offices maintains the same level of security and procedures to address special issues, including data-transfer agreements, secure transmission procedures, and encryption. Additional safeguards are also followed, including: maintenance of minimal data on home computer, use of electronic screen savers, and password control at home.

Paper Record Security

_____ *(Firm or Registry)* maintains the confidentiality of paper records by:

❍ ❍ Restricting access to data-storage areas, the use of locked file rooms or cabinets in limited-access areas, a forms tracking log for any external disclosures, and a sign-out system for internal use of data.

❍ ❍ Development and implementation of policies by institutions for the secure transport of information from one physical location to another.

❍ ❍ Assuring confidentiality of written evidence that a patient is on a specific research study; for example, logs or lists of screened individuals or participants should not be left out on desks or in other open-access areas.

❍ ❍ Safeguarding of ancillary records, e.g., pharmacy records, data on patients screened for clinical trials participation, etc.

❍ ❍ Situating FAX machines in secure or limited-access areas; use of pre-coded phone number to eliminate dialing errors; cover sheets so data are not physically exposed; testing FAX machines to insure correct number and function; and de-programming FAX memory storage after use to prevent recovery of confidential information.

❍ ❍ Employing established shredding procedures for disposal of documents after use.

❍ ❍ Hardcopy information of sensitive information sent outside of the department is protected.

Re-release of _____ *(Registry)* Data Files

_____ *(Firm or Registry)* does not release any _____ *(Registry)* data files to any one without written consent of the Registry Director or designee.

A written consent is required every time a data request is received, even if the requester has obtained previous approval or if new data are added to a data file that was previously approved for release.

_____

Signature

_____

Typed Name

_____

Title

_____

Date