Georgia Department of Public Health
Confidentiality Agreement / Checklist

To be completed yearly by all project staff. If an activity is not applicable to an individual's duties, mark N/A beside the requirement.

As a **Grantee** I understand that I will be exposed to some very privileged protected health information. Examples of such information are medical conditions, medical treatments, demographics, contact information, and finances. The patient's right to privacy is not only a policy of the State of Georgia, but is specifically guaranteed by statute and by various governmental regulations.

I understand that intentional or involuntary violation of the confidentiality policies is subject to appropriate disciplinary action(s) that could include being discharged from my position and/or being subject to other penalties. By checking the following statements I further agree that:

I. General Confidentiality Policies

- ❑ I understand that I am personally responsible for the validity, accuracy, and security of the data I collect.
- ❑ I understand that I am responsible for challenging unauthorized users of the data. I will report security irregularities to the **DPH Linkage Coordinator**.
- ❑ I understand that I am responsible for:
- ❑ Protecting my individual files, workstations, and computers that contain confidential data, including protection from computer viruses and from extreme temperatures (laptops)
- ❑ Preventing unauthorized access to or use of my passwords and codes that allow access to confidential information or data. I will immediately report lost, stolen, or compromised passwords or codes to the **DPH Linkage Coordinator.**
- ❑ Safeguarding my keys to offices and filing/storage cabinets. I will immediately report lost or stolen keys to your **Agency Designee**.
- ❑ I understand that I am bound by these policies, even upon resignation, termination, or completion of my activities.

II. Offices

- ❑ My office is kept locked when it is not occupied, if it contains any confidential information, keys, or codes.
- ❑ I know the location of all of my keys, and they are maintained on my key ring or in a location that is not easily identifiable.
- ❑ I always store items with patient identifiers in a locked filing/storage cabinet, and not on my desk, when not in use.
- ❑ Visitors do not enter my office until I have secured all documents that contain confidential information.
- ❑ If I have external visitors, I escort them to and from the area(s) in which their business is to be conducted. I ensure that the visitor, whether client or outside professional, is brought to a private area before beginning any in which confidential patient information is discussed.
- ❑ I report any special circumstances that may affect the security of offices (e.g., broken locks) immediately to your **DPH Contract Monitor (Standard A11).**

III. Mail

- ❑ I am aware that mail addressed to a specific employee is to be opened only by that person or his/her designee within the Program.
- ❑ I ensure that any mail I send that contains confidential information contains only the minimum information necessary, if possible is de-identified, or does not have reference to diagnoses.
- ❑ Any mail I send that contains confidential information is sent in a sealed and taped internal envelope that is addressed (including return address), stamped "confidential," and placed inside an external envelope that has complete mailing and return mail addresses. Mail containing confidential information is sent via a service that is traceable (registered, certified, or courier)
- ❑ When mailing hardcopies with identifiers, I send no more than 100 names/identifiers per envelope.
- ❑ I confirm receipt of any confidential package I send.
- ❑ I maintain a log of all confidential items I mail and the date, as well as notification of receipt. I review this log weekly to verify entries are complete.

IV. Telephone/Fax/Email

- ❑ I discuss confidential information by telephone only after ascertaining that the contact is legitimate.
- ❑ Any call I make involving confidential information is made from a private area where the conversation will not be overheard.
- ❑ I never leave personal identifiers related to confidential records on voicemail messages. My outgoing voicemail message requests that callers not leave confidential information in a voicemail message.
- ❑ I never send information by fax. I do not email documents.
- ❑

V. Handling of Paper Records

- ❑ When not in use, I store all documents with confidential information in a locked filing/storage cabinet inside a locked office.
- ❑ When confidential information is taken from a secured area:
- ❑ I transport confidential information inside a secure container
- ❑ I transport only the minimum amount of information needed for completing the task and are, when possible, coded to disguise any term that could easily be associated with the patient diagnoses.
- ❑ Confidential records may <u>not</u> be taken home/hotel unless there is an unpreventable circumstance (such as an unexpected storm, accident, etc.). In the event of such an emergency, I will notify my supervisor as soon as possible, will keep the records in a secure location inaccessible by others, and will ensure that only I have knowledge of or access to the confidential information.
- ❑ I always shred documents containing confidential information when it is no longer needed. I understand that I must ensure that the shredding does not produce readable lines of data.

VI. Maintaining the Security of Computer Workstations and Laptops ❑ My computer is protected with a password, in addition to a network/email sign-on password.

I do not keep my passwords where they can be seen or found by others.

- ❑ The screens of my desktop and laptop computers are always situated so that they are not visible to non-authorized personnel or through windows. If needed, I use a privacy screen.
- ❑ Unless required by travel, I always store my laptop in a secure, locked location in the office when not in use. (Separate requirements for securely storing confidential electronic data are in Section VII). When using a laptop in the field, it is never left out of my sight.
- ❑ I recognize that wireless internet capability is a security hazard. Therefore, when operating any computer equipped with wireless (WI-FI) capability:
- ❑ Wireless capability is **disabled** (e.g. "disable radio") before any removable media containing confidential information is inserted/connected to the computer.
- ❑ I always remove any flash drive or other media containing confidential information from the computer before enabling or utilizing wireless capability.
- ❑ I never store confidential data on the computer hard drive.

VII. Handling of Electronic Files

- ❑ I may store electronic files with confidential information only if: 1) they are encrypted and stored on a removable media; 2) they are encrypted using PGP 3072-bit encryption (or other approved encryption); and 3) the removable media with encrypted information is kept in a locked secure location when not in use. In addition, I store any removable media for a laptop computer in a secure location apart from the laptop.
- ❑ I electronically transfer sensitive data only if it is encrypted using PGP 3072-bit encryption (or other approved encryption).

VIII. Record Retention

❑ I always store confidential electronic and paper records securely until they are destroyed. ❑ Clients older than 18 years of age health records are to be kept by the healthcare provider for a period of 10 years. ***O.C.G.A. 31-33-2 (a)(1)(A)***

IX. Release of Statistics and Other Program Data

- ❑ I never release confidential data to the general public.
- ❑ All media inquiries should be handled according to agency written protocol and policy.

XI. Breach of Security

I understand what constitutes a potential breach of security and will report any such problems or potential problems to the Linkage Coordinator. I agree to abide by the Georgia Department of Public Health Confidentiality Agreement. I have received, read, understand, and agree to comply with these guidelines.

<u>Warning:</u> Persons who reveal confidential information may be subject to legal action by the person about whom such information pertains as well as be subject to appropriate disciplinary action up to and including termination from employment.

Signed: _____ Date: _____
(Linkage Coordinator)

Signed: _____ Date: _____
(Program Manager)

Agency: _____

Supervisors: After completion and review of checklist, submit to the DPH Linkage Team.