**Appendix A**: CDCPB S&C Training Checklist

**Montana Epidemiology and Scientific Support Bureau Confidentiality Checklist**

As a Epidemiology and Scientific Support Bureau (ESSB) or Communicable Disease Control and Prevention Bureau (CDCPB) employee, subcontracted employee, student, intern or visiting professional, I understand that I may encounter protected patient health information. The patient’s right to privacy is not only a policy of the Department of Public Health and Human Services but is specifically guaranteed by state statute and governmental regulations [Section 1(c)].

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

* + - 1. **General Confidentiality Policies Initials \_\_\_\_\_\_\_\_\_\_\_**
* 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 protected health data and I will report security irregularities to my supervisor.
* 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 cold or hot temperatures.
* I understand I am responsible for keeping a copy of the ESSB S&C Policy readily available.
* I understand that I am bound by these policies, even upon resignation, termination, or completion of my activities.
  + - 1. **Offices Initials \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* Confidential information, keys and/or passwords are secured in my office when it is not occupied.
* I know the location of all my keys, and they are maintained on my key ring or in a location that is not easily identifiable.
* I always secure items with patient identifiers in a secure 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.
* I will prevent 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 my supervisor.
* I will safeguard my keys to offices and filing/storage cabinets. I will immediately report lost or stolen keys to my supervisor
* I report any special circumstances that may affect the security of offices (e.g., broken locks) immediately to my supervisor.
  + - 1. **Mail Initials \_\_\_\_\_\_\_\_\_\_\_**
* I am aware that mail addressed to a specific CDCPB or ESSB employee or non-DPHHS user is to be opened only by the person it is addressed to.
* 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 specific health conditions.
* 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).
  + - 1. **Telephone/Fax/Email Initials \_\_\_\_\_\_\_\_\_\_\_**
* I never send information that contains personal identifiers by email (even with encryption
* I only send information that contains confidential personal identifiers by fax when the recipients fax machine is in a secure location. 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, such as an office or work area, where the conversation will not easily be overheard.
* I never leave personal identifiers related to confidential records on non-confidential voicemail messages.
  + - 1. **Handling of Paper Records Initials \_\_\_\_\_\_\_\_\_\_\_**
* When not in use, I store all documents with confidential information in a secure location within a secured area.
* Confidential records should not be taken home off-site unless there is an unpreventable circumstance (for example, a public health emergency, such as a pandemic). In the event of such an emergency, I will notify my supervisor as soon as possible, keep the records in a secure location inaccessible by others, and ensure that only I have knowledge of or access to the confidential information.
* When photocopying confidential information, I always ensure that the document cannot be viewed by others.
* I always shred documents containing confidential information when it is no longer needed with a cross-cutting shredder. I understand that I must ensure that the shredding does not produce readable lines of data.
  + - 1. **Maintaining the Security of Computer Workstations Initials \_\_\_\_\_\_\_\_\_\_\_**
* My computer is protected with a power-on and screensaver 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 situated so that they are not visible to unauthorized personnel. If needed, I use a privacy screen.
* When accessing confidential information on the computer work station, I lock the work stations when not in use and I am away from my desk.
* I understand that I am responsible for maintaining the virus definitions and other updates to my laptop (Off-site staff are also responsible for this maintenance for desktop computers).
* Unless required by travel, I always store my laptop in a secure location in the office when not in use.
* 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 diskette 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
* If repairs of computer equipment are needed, I understand that this must be done by DPHHS TSD, or if outside assistance is needed, this activity is supervised by the DPHHS TSD once permission is granted from my supervisor.
* I give outdated computer equipment only to the DPHHS TSD to ensure proper disposal.
  + - 1. **Handling of Electronic Records Initials \_\_\_\_\_\_\_\_\_\_\_**
* I store electronic files containing confidential information only in designated secure folders, which are only accessible by authorized staff. I understand that files with confidential information are never to be stored on the hard drive of any individual computer.
* I may store electronic files with confidential information on removable media only if: 1) they are DPHHS TSD approved encryption; and 2) 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.
* Diskettes and other storage media I use: 1) contain only the minimum information needed; 2) are encrypted using DPHHS TSD approved encryption; 3) are never taken into the field without appropriate encryption; and 5) are permanently deleted following completion of the task.
* I electronically transfer sensitive data only if it is encrypted using DPHHS TSD approved encryption.
  + - 1. **Record Retention Initials \_\_\_\_\_\_\_\_\_\_\_**
* I always store confidential electronic and paper records securely until they are destroyed.
* I always destroy confidential paper records by shredding using a cross-cut shredder.
* I destroy confidential electronic records with guidance from DPHHS TSD.

**9. Release of Individual-level Data/Release of Records Initials \_\_\_\_\_\_\_\_\_\_\_**

* I do not release names or personal identifiers to any persons or facilities unless as specified in Section X of the ESSB S&C Policy.
* If I am responsible for preparing and/or releasing reports/statistics, I fully understand all of the procedures outlined in the ESSB S&C Policy and I always obtain the appropriate releases and Confidentiality Agreements, as specified in the ESSB S&C Policy.

**10. Release of Statistics and Other Program Data Initials \_\_\_\_\_\_\_\_\_\_\_**

* I never release confidential data to the general public.
* I direct all media requests to my supervisor who will work with the Public Information Office.
* I always direct requests for data that are not in standard published reports to my supervisor.
* If I am responsible for preparing and/or releasing reports/statistics, I fully understand all the procedures outlined in Sections M and N of the ESSB S&C Policy and I always obtain the appropriate releases and confidentiality agreements as specified in the policy.

**11. Surveillance Program-Specific Confidentiality Requirements Initials \_\_\_\_\_\_\_\_\_\_\_**

* If working with HIV/STD data, I have reviewed and understand the requirements specified in Section O of the HIV/AIDS Surveillance Program Confidentiality Policy.

**12. Breach of Security Initials \_\_\_\_\_\_\_\_\_\_\_**

* I understand what constitutes a potential breach of security and will report any such problems or potential problems to my supervisor.

**Warning: Persons who reveal confidential information may be subject to legal action by the person about whom such information pertains.**

*I agree to abide by the Epidemiology and Scientific Support Bureau Security and Confidentiality Policy. I have received, read, understand, and agree to comply with the guidelines.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Employee Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Supervisor Date