MONTANA DPHHS Healthy People. Healthy Communities. Department of Public Health & Human Services	**STATE OF MONTANA** **DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES**

Title:	Communicable Disease Control and Prevention Bureau Security and Confidentiality Policy (CDCPB S&C)
Effective Date/Details:	Pages: 1–17
	Effective Date: March 2014
	Revision Date: 10/15/2018
	Rescission Date:
	Attachments: Appendices A–F

I. PURPOSE

A. The Communicable Disease Control and Prevention Bureau (CDCPB), a bureau in the Department of Public Health and Human Services (DPHHS), ensures that all confidential information collected, used, and archived by programs within the Bureau remains secure through compliance with the CDCPB Security and Confidentiality Policy (CDCPB S&C). The procedures and practices outlined in this policy are consistent with more general confidentiality policies of DPHHS.

The CDCPB S&C outlines the appropriate use and protection of confidential information, protected health information, potentially identifying information, and analysis and presentation of non-aggregated small denominator and numerator data, for justifiable public health purposes. Examples of justifiable public health use by a CDCPB program include, but are not limited to: disease surveillance, disease investigation coordination and reporting, data analysis, and report writing.

The CDCPB S&C complies with Montana law to ensure transparency of government. The Policy does not restrict the collection, use, and release of aggregate summary statistics or data pre-approved by the Overall Responsible Party (ORP). The Policy complies with Montana law to protect confidentiality. The Montana legal standard is that it should not reasonably be possible to identify an individual using aggregate summary statistics.

The ORP may waive policy restrictions when they determine that it is not reasonable to identify an individual from aggregate summary statistics or the public health benefit outweighs any potential harm that may come from the exemption. When a data request is not covered in the CDCPB S&C Policy, the appropriate Section Supervisor, ORP, and

State Epidemiologist may review and authorize a data release when the public health benefit outweighs any potential harm that may come from the release.

B. All authorized users of CDCPB confidential information must follow these policies and procedures. Categories of persons who are authorized to use or handle CDCPB confidential information include: CDCPB staff, DPHHS Technology Services Division (TSD) staff, other DPHHS staff, and authorized non-DPHHS users (e.g., federal funders, auditors, students, interns, or others) who obtain authorization from the CDCPB Chief.

DPHHS TSD staff must comply with TSD policies and CDCPB S&C policies.

C. This policy complies with:
1. The Centers for Disease Control and Prevention's (CDC) *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action* (CDC Data S&C) document.
2. Montana Code Annotated
   a. MCA 50-16-603. Confidentiality of health care information
   b. MCA 50-18-109. Permissible release of information concerning infected persons
3. HIPAA 164.530

II. POLICIES

A. Personnel Clearance and Authorization

1. The Overall Responsible Party (ORP) is a DPHHS management employee who has the ultimate responsibility to ensure compliance with the CDCPB S&C.
   a. The ORP maintains, evaluates, and updates the CDCPB S&C.
   b. The ORP is the CDCPB Chief.
   c. The ORP may delegate action to CDCPB staff.
2. Authorized users of CDCPB confidential information are classified into four categories for the purpose of clearance and authorization processes. The categories are: CDCPB staff, DPHHS TSD staff, DPHHS non-CDCPB staff, and non-DPHHS users including students and interns.
3. Clearance and Authorization
   a. User categories
      i. CDCPB staff
         (a) The scope of work delegated to an authorized user determines their access and use of CDCPB confidential information.
            (1) CDCPB staff have different levels of access to confidential databases or hardcopy files although they are responsible to maintain the security of any confidential information they encounter in the course of their work.
            (2) The CDCPB Chief, or data owner designated by the Chief, determines the access level, ranging from full modification to view only, for electronic data systems and drives.
      ii. DPHHS TSD staff

(a) The DPHHS TSD administers the networks that house electronic CDCPB confidential information.
(1) DPHHS TSD network administrators secure written permission from the CDCPB Chief, or data owner designated by the Chief, prior to permitting any authorized person electronic access to network areas that contain confidential information.

iii. DPHHS non-CDCPB staff
(a) The CDCPB Chief may authorize a DPHHS non-CDCPB user if the Section Supervisor determines that the intended use of CDCPB confidential information meets the standard of an express and justifiable public health need. The user must complete all designated training assigned by the CDCPB Chief and sign all designated agreements.

iv. Non-DPHHS authorized users including students and interns
(a) The CDCPB Chief may authorize a non-DPHHS user if the CDCPB Chief determines that the intended use of CDCPB confidential information meets the standard of an express and justifiable public health need. The user must complete all designated training assigned by the CDCPB Chief and sign all designated agreements.

b. Upon resignation or termination, all authorized users must complete and sign the *Resignation/Termination Checklist* (Appendix A). In the Checklist the user certifies that they:
i. do not possess any confidential information in the forms of paperwork, diskettes, or other media;
ii. returned all keys to secured areas;
iii. returned identification badges; and
iv. acknowledge their obligation to maintain the security of confidential information after employment and may be subject to legal action if they fail to meet this obligation.

B. Authorized User Training

1. All authorized users of CDCPB confidential information.
   a. Each user completes CDCPB S&C training prior to receiving access to confidential information and annually thereafter.
   b. Each user signs designated agreement after training. (Appendix B)
   c. Each user completes the DPHHS Health Insurance Portability and Accountability Act (HIPAA) training upon hire.
2. DPHHS TSD staff
   a. DPHHS TSD network administrators receive TSD training and review security and confidentiality policies and procedures provided to all technology staff with access to confidential information.
   b. TSD staff who support CDCPB receive CDCPB S&C training and sign the corresponding confidentiality agreement.
3. The ORP is responsible for monitoring and retaining authorization and training documentation, including the original signed agreement, for all users during their authorized access period.

a. The ORP may delegate this responsibility to Section Supervisors or Program Coordinators.
b. The authorized user retains a copy of the signed agreement and ORP or designated delegate retains the original.
c. When an employee resigns or is terminated, the ORP, or their designee, submits the documentation to the respective Section Supervisor. The Section Supervisor ensures that the documentation is forwarded to the user's supervisor.
    i. The user's supervisor incorporates it into the personnel record
d. The ORP retains documentation for all non-DPHHS authorized users.

C. Authorized User Responsibilities

1. An authorized user protects individual files, workstations, and computers that contain confidential data. The protection of electronic devices includes preventing exposure to extreme hot or cold temperatures and compromise by computer viruses or malware.
2. An authorized user protects passwords and codes.
3. An authorized user immediately reports incidents of lost, stolen, or compromised passwords or codes to their supervisor.
4. An authorized user immediately reports incidents of lost or stolen keys to offices and filing or storage cabinets to their supervisor.
5. An authorized user has the CDCPB S&C Policy readily available (hardcopy or electronic format).
6. An authorized user challenges an unauthorized user and reports the security irregularity to their supervisor.
7. An authorized user monitors and evaluates data for quality and accuracy during collection, management, and analysis.

D. Data Integrity

1. An authorized user must comply with media policies and procedures.
2. An authorized user must comply with data release policies and procedures and adhere to *Guidelines for the Release of Public Health Data Derived from Personal Health Information* as provided by the State of Montana's Office of Epidemiology and Scientific Support (OESS). Compliance may be exempted with approval from the CDCPB Chief. (References and Related Materials, section V part C)

E. Case Records and Other Hardcopy Confidential Information

1. All records and other hardcopy information that contain potentially identifying or confidential information remain in a secured area or in a prescribed secure manner per CDCPB S&C protocols at all times.
2. During a workday interval, all records and other hardcopy information that contain potentially identifying or confidential information remain in a secured locked location.

F. Electronic Record and Database Systems

1. Servers belonging to a closed Local Area Network (LAN) contain electronic files of identifying or confidential data.

a. Access to CDCPB data or databases housed in the LAN is limited to authorized users.
b. The file servers are located in secured server rooms or authorized remote locations.
c. Databases and files containing confidential information are stored in file share volumes separated according to program area components.
d. Access to specific drives is regulated by Windows domain security policies to ensure that access to confidential information is limited only to those authorized users.
e. Domain accounts are password protected and are enabled for login.
f. Individual workstation computers with access to the secure data network are protected with *Encryption Anywhere*© passwords and password-protected screen savers.

G. Secure Physical Work Space

1. Workspaces at DPHHS
   a. CDCPB workspaces do not have feasibly accessible ground level windows.
   b. CDCPB staff lock unoccupied areas that contain confidential information when the area is not in use.
   c. Section Supervisors designate Administrative Assistants who maintain copies of all office keys in a secure location.
   d. CDCPB staff configure workspaces to ensure that confidential information on computer screens is not visible to any person within or passing by workspaces.
2. Remote Workstations and Computers
   a. Only another worksite office can serve as an authorized remote work location.
      i. A residence is not an authorized work location.
   b. Specific software and special configuration limit accessibility on each authorized machine.

H. Confidentiality and Coordination by CDCPB with other Montana State Programs and Departments

1. CDCPB maintains security of confidential information when coordinating with other DPHHS programs, or other partners, for surveillance or other justifiable public health need.

I. Breach in Confidentiality

1. Infractions related to inappropriate access or disclosure of confidential information may result in disciplinary action, termination of employment, loss of professional licensure, and/or legal prosecution.

J. Policy Monitoring and Review

1. The ORP monitors and reviews the CDCPB S&C policy to ensure and certify that it meets all security and confidentiality requirements for each CDCPB program.
   a. The ORP may delegate monitoring and reviewing activities.
2. Specific policy monitoring and review criteria include:

a. Review the roster of authorized users to ensure that access complies with CDCPB S&C policy annually.
b. Ensure that ORP or Section Supervisors conduct a compliance review with each authorized user to:
    i. review the CDCPB S&C;
    ii. identify and monitor worksite issues which may include on-site review with the authorized user;
    iii. verify that CDCPB S&C training is complete. (See Appendix B.)
c. Ensure all authorized users complete CDCPB S&C training annually.
d. Ensure maintenance of documentation pertaining to CDCPB S&C Policy.
    i. Section Supervisors retain agendas for staff and other meetings and attendance rosters for meetings and trainings.
    ii. Section Supervisors include maintaining security for confidential information as an agenda topic at staff meetings on a regular basis.

3. The ORP revises the CDCPB S&C Policy annually to ensure it complies with the CDC Data S&C requirements and comports with applicable MCA.

III. PROCEDURES AND RESPONSIBILITIES

A. Physical Offices/Workstations/Storage Areas

1. Construct physical conditions to comport to the following criteria.
    a. No office in which confidential information is stored, network computers are housed, or electronic files are accessed can feasibly be entered through a ground level window.
    b. Workspace configurations ensure that confidential information on computer screens or present in workstations is not visible to unauthorized personnel who are in or passing by workspaces.
        i. Desktop monitor placement ensures that confidential information is not visible to unauthorized personnel who are in or passing a work area.
        ii. Computer screens are not visible through a ground level window.
        iii. Privacy screens effectively limit any viewing by others when it is impossible to limit viewing through computer placement.
        iv. Authorized users in the field place laptop computers so as to prevent others from viewing screen.
            (a) Authorized users keep laptop in their sight at all times.
2. Do not use or store computers in conditions of extreme heat or cold exposure.
3. Store all items with confidential information in locked filing or storage cabinets. Do not leave items unsecured on desks or work surfaces.
4. Maintain the keys in a secure location.
    a. Keep keys on a key ring in a location that is not easily identified.
    b. Keep individual keys in a location that is not easily identified.
5. Ensure that no one enters a work area that may contain confidential information when a staff person is out of the office.

a. Only management can authorize use of a workspace.

6. Immediately report any special circumstances that impact the security of offices (e.g., broken locks, ground level windows, etc.) to a supervisor.
7. Cleaning crews and other building maintenance personnel may only be escorted to work areas that contain confidential information during the hours personnel who work in these offices are present or a management designee is available.
    a. Cleaning and maintenance crews do not have access to offices that may contain confidential information outside of normal operating hours, unless approved by the Section Supervisor.

B. Visitor Management

1. All visitors (whether CDCPB personnel visiting a coworker, other DPHHS staff, or external visitors) must obtain permission to enter offices where confidential information is handled.
    a. Staff escort a visitor to a public area until permission can be obtained.
2. Secure confidential information is out of sight prior to inviting individuals into an office.
3. Never discuss confidential information outside a private area. Ensure that it is not possible to overhear conversations.

C. Postal Mail Confidentiality

1. Manage incoming mail to the appropriate recipient to ensure security of confidential information.
    a. DPHHS staff route postal mail to the addressee.
        i. CDCPB staff may designate another CDCPB staff to receive their addressed mail.
    b. DPHHS staff direct postal mail not addressed to CDCPB staff or authorized user to the Section Supervisor or Program Coordinator.
    c. The staff who opens the mail date stamps the document.
2. Authorized users comply with the following restrictions when they mail confidential information.
    a. Line lists do not contain identifiers pertaining to a disease or condition.
    b. Send no more than 100 names and/or personal identifiers per envelope.
        i. CDCPB staff hand deliver lists that contain over 500 names/personal identifiers to their recipient(s).
    c. Provide instructions to maintain confidentiality for reporting providers. (Appendix D)
3. Authorized users manage outgoing mail to ensure security of confidential information.
    a. Use a double envelope system to mail confidential information.
        i. Double envelope system procedure:
            (a) Place address and return address on both envelopes.
                (1) Do not place any disease or condition identifier on the outside envelope.
                (2) Stamp inside envelope “CONFIDENTIAL.”

(b) Place confidential information into inside envelope that is sealed, taped, addressed, and stamped "CONFIDENTIAL."
(c) Insert inside envelope into second, outside, envelope.

b. Sender verifies that the information has been received.
   i. Use a return receipt for any confidential package.

4. Authorized users maintain a mailing log.
   a. Include confidential items mailed, date sent, and notification or verification of receipt.

D. Telephone Communication

1. Never leave personal identifiers or confidential information on non-confidential voicemail.
2. Ensure, to a reasonable degree, that phone contact is legitimate before communicating confidential information.
3. Make telephone calls that contain confidential information from a private area where the conversation will not be overheard.

E. Email, Text, and Fax Communication

1. Email and text
   a. Never email or text confidential information, including medical record numbers.
   b. Never email or text encrypted confidential information.
2. Fax
   a. Use procedure in Appendix E to communicate confidential information by fax machine.
   b. Ensure that recipient's fax machine is located in a secure location prior to any transmission of confidential information to that recipient.

F. Management of Records and Other Hardcopy Confidential Information

1. Store all documents with confidential information in locked filing or storage cabinets within offices that are locked when not in use.
2. Ensure all confidential information is secured at the close of business each day.
3. When removing confidential information from a secured area:
   a. Transport confidential information inside a secure container (e.g., locked briefcase or backpack).
   b. Ensure that hardcopy documents contain only the minimum amount of information needed.
   c. Code documents to disguise any term easily associated with a disease.
   d. Ensure that documents with personal identifiers do not contain information related to a disease identifier (e.g. HIV/AIDS) and, conversely, documents with a disease identifier do not contain information related to a personal identifiers.

G. Photocopying

1. Use caution when photocopying confidential information.
2. Ensure that confidential information cannot be viewed by others during duplication.
3. After completing duplication of any confidential information, clear the copy machine by making a single copy of a blank page.

H. Shredding and Disposal

1. Use cross-cutting shredder to destroy paper documents or compact discs (CD) containing confidential information.
2. Ensure that shredded paper does not contain readable lines of confidential information.

I. Work in the Field

1. Taking confidential information from work to home is not acceptable within normal CDCPB activities. Avoid this practice whenever possible.
2. When direct travel between usual workplace and field site is impossible or unadvisable due to severe weather or other unpreventable emergencies, staff may take confidential information with them overnight (e.g., home or motel) under the following conditions:
    a. Records are concealed in a secure location that is not accessible to others.
    b. Only the authorized user has knowledge of and access to the confidential information.

J. Maintaining the Security of Computer Workstations

1. Computers with access to confidential information must have network log on and screen saver passwords.
    a. All passwords are to be at least six characters in length and not easily guessed.
        i. Do not use spouse names, initials, children/pet names, or a dictionary word.
    b. Change computer passwords every 60 days or when there is suspicion a password is compromised.
    c. Do not document passwords where they can be seen or found by others.
2. Update computer virus protection definitions weekly and upload operating system updates when they are released.
    a. DPHHS TSD manages updates for the networked computers.
    b. Field personnel ensure laptops have current updates by logging onto the Montana State network and running all updates.
3. Unless required because of travel, store laptops in a secure and locked location within the CDCPB or field office when not in use.
    a. Do not store confidential information on the hard drive of laptops.
    b. Store encrypted removable media in a separate location which is apart from the laptop when not in use.
4. Wireless internet capability is a security hazard. Exercise special precautions when using confidential information on a computer equipped with wireless (Wi-Fi) capability:
    a. Do not store confidential data on the computer hard drive.
    b. Disable wireless capability while any removable media containing confidential information are inserted or connected to the computer (“Disable” Wi-Fi).
    c. Remove all media containing confidential information prior to enabling or utilizing computer wireless capability.
5. Maintain security of confidential information when performing computer equipment repairs by minimizing use of unauthorized personnel.

   a. CDCPB staff and DPHHS TSD staff attempt to correct the problem.
   b. If technology consultants outside the DPHHS are needed, DPHHS TSD obtains permission from the appropriate Section Supervisor.
   c. Remove all removable media containing confidential information prior to repair.
6. Give outdated computer equipment to the DPHHS TSD technician who ensures that all confidential material is completely removed from any internal hard disks.
   a. The technician reformats and securely overwrites all hard disks and storage diskettes to prevent data retrieval.
   b. The secure reformat date for each surplus workstation is recorded in the Comprehensive Computing Materials Inventory database and submitted with surplus requests made to the Department of Health and Hospitals.

K. Handling of electronic records

1. Confidential electronic files, including data sets with personal identifiers must be stored on designated drives on a secure server (e.g., H:\EPI-Private\).
   a. Do not maintain content from these drives on an individual computer hard-drive.
   b. Personnel who need access to existing files/folders on the secure server, or who need to establish a private folder for confidential data, should request this through the DPHHS TSD.
2. Do not store confidential information from any source on the hard-drive of any computer.
3. Confidential electronic files for personnel without access to the LAN are maintained as follows:
   a. Electronic files containing confidential information, including data sets with personal identifiers, are encrypted and saved on removable media.
   b. Encrypt data using PGP 3072-bit encryption (or other high-level encryption software approved by the program manager) and protect with passwords.
   c. Store removable media containing the confidential encrypted data in a locked, secured location that is not feasibly accessible through a ground level window.
4. Comply with the following required criteria for all diskettes and other storage media that contain confidential information, including data sets with personal identifiers.
   a. Include only the minimum amount of information necessary to accomplish assigned tasks.
   b. Encrypt using PGP 3072-bit encryption (or other high level encryption software approved by DPHHS TSD) and store in locked container when not in use.
   c. Electronically “wipe” or physically destroy diskette or storage media immediately upon completion of the assigned task. Merely erasing is not sufficient for disposal of confidential information.
   d. Never take into the field unless encrypted using PGP 3072-bit encryption (or other high level encryption software approved by the Department of Administration and DPHHS TSD).
5. Electronic transfers of sensitive data will incorporate the use of PGP 3072-bit encryption (or other high level encryption software or method approved by the Department of Administration and the DPHHS TSD.
6. DPHHS TSD performs backup of all critical files daily.

L. Record Retention

1. Store all electronic and paper records according to CDCPB S&C until they are destroyed.
2. Destroy records according to the CDCPB S&C procedures in section III part H (paper records) and section III part K(c) (electronic files).

M. Release of Statistics and Other Program Data

1. Confidential data, including data sets with personal identifiers, maintained by the CDCPB are not released to the general public.
2. Confidential data, including data sets with personal identifiers, maintained by the CDCPB may be released to the local health department where the data originated or to the local health department responsible for conducting the disease investigation or implementing control measures.
3. All media requests for interviews or statements must be approved by the Section Supervisor and follow DPHHS media policy.
4. Requests for data, not otherwise contained in publically available reports or publications, must comply with CDCPB S&C.
    a. All requests must comply with the following criteria.
        i. The request must be routed through the Section Supervisor.
        ii. The Section Supervisor must approve the request.
        iii. Completed data requests must comply with the State of Montana's Office of Epidemiology and Scientific Support's (OESS) *Guidelines for the Release of Public Health Data Derived from Personal Health Information*, unless exempted by the ORP. (References and Related Materials, section V part C)
5. Other requests
    a. The Section Supervisor may consider and approve a data request for potentially sensitive or identifiable aggregate data (i.e., zip code, block, or other potentially small-denominator data).
    b. The ORP and Section Supervisor review other data requests to determine whether the requests meet the standards for reasonableness and public health benefit.
    c. A data request proposing use of identifiable public health data outside of the grant-funded activities as outlined in CDC grant deliverables may require an IRB review. The Section Supervisor, ORP, and the State Epidemiologist must review the request.

N. Release of Individual-level Data or Release of Records

1. Outside the scope of regular public health duties to identify cases of reportable conditions and to implement control measures, the release of individual-level information, with or without identifiers, occurs in very limited circumstances. Generally, the circumstance is when individual-level information is released to the person or entity who provided the information or persons responsible for implementing the control measures as outlined in MCA 50.16.603.
    a. Responses to requests from providers (physicians, facilities, counseling/testing sites, Ryan White providers) for data with personal identifiers must be generated by CDCPB and may be released following these criteria.
        i. Section Supervisor and ORP authorize the release.

ii. CDCPB staff have provided the site with recommendations on handling and maintaining confidential information.
iii. The requested information originated with the requesting provider.
(a) Only the Section Supervisor and ORP may authorize release information in the situation where:
(1) the requesting provider did not originate the information
(I) example: request for vital status
(2) it is unclear the requesting provider is the original reporter of the information.
iv. Information for an institution that originally provided the data is released only to the individual(s) responsible for reporting for that institution.

2. Court orders, subpoenas, or other requests for individual information are referred to the Section Supervisor. If needed, the Section Supervisor then refers the issue to the ORP or State Epidemiologist. In these instances, information is granted only to the extent required by law.
3. With the approval of the Section Supervisor and ORP, an individual's personal records may be released directly to that individual, or their representative.
a. S/he must sign a *Request for Personal Health Information* and a staff member must verify the individual's identity. The Section Supervisor and ORP must approve the *Release of Information*. (Appendix C)
b. If the Section Supervisor and ORP affirm the request, the individual receives the requested information. If the request is denied, the individual receives a letter detailing the reason for denying the request.
c. The individual may amend and resubmit the request.
4. Wherever it is reasonably and legally feasible to do so, CDCPB accommodates an individual's request to communicate via alternate methods and/or locations.
5. The Section Supervisor and ORP review other data requests that include personally identifiable information to assess risks and benefits of releasing the information. Generally, information is only released to be used for public health prevention and investigation activities (MCA 50-16-603). For consideration, data requests must:
a. demonstrate a need for names;
b. obtain and comply with any necessary IRB approval(s); and
c. include a signed confidentiality agreement.

O. Confidentiality Specific to the HIV Surveillance Program (HSP)

1. The main aims of the HSP are to identify HIV cases, link persons to care, and implement control measures to prevent HIV transmission. To achieve these goals, the HSP must share confidential information with local and state public health entities and health care providers. Disclosure of confidential information during the investigation, prevention, and implementation of control measures is done in compliance with Montana Code Annotated (Title 50, Chapters 16 and 18) and the Administrative Rules of Montana (Chapter 37.114).
2. Contact/Referrals
a. CDCPB staff attempt to conduct all initial contact with providers and/or local health jurisdictions.

b. CDCPB staff facilitate coordination between programs, for instance staff coordinate with TB program to refer TB/HIV or TB/AIDS cases to the TB program. (Section II part P)

3. Surveillance Records/Case Reports
   a. Use case report forms to submit original and updated case data, with the exception of non-electronic lab reports.
   b. After database entry, store and maintain all surveillance case report records in a secured CDCPB room/office.
      i. Store documents in paper and/or electronically scanned format indefinitely.
      ii. Dispose of unneeded documents in a secure procedure.
         (a) Shred duplicate case reports after entering data into the surveillance database and the report form filed.
   c. For HSP, the HIV Surveillance Coordinator reports cases to CDC by electronic transfer, using CDC high-level encryption, without personal identifiers each month. Names and personal identifiers are never released to the CDC.
   d. When establishing new DPHHS sites for program activities, program staff provide procedures for coordination to maintain security of confidential information.
      i. For HSP surveillance or when health care providers inquire about how to report, the HIV Surveillance Coordinator:
         (a) discusses confidentiality responsibilities of both the reporter and the CDCPB;
         (b) informs the provider about methods of reporting;
         (c) gives the provider a copy of *Recommendations for Maintaining Confidentiality* (Appendix D); and
         (d) supplies case report forms with appropriate address to providers who report by mail or fax.

P. Confidentiality and Coordination by CDCPB with other DPHHS Programs

1. Registry matches for reportable conditions:
   a. The Vital Records (birth and death registries) match and certain other matches require CDCPB Surveillance personnel to sign Confidentiality Forms from the program providing the database to be matched. In addition to the confidentiality policies of CDCPB, persons involved in matching to databases outside the CDCPB Program are bound by the specific confidentiality policies of the partner program.

Q. Security Breaches

1. A security breach can be defined as, but is not limited to:
   a. Hardcopy or computer media containing confidential material is lost or stolen.
   b. Hardcopy or computer media containing confidential material has been given or shown to a person who is not authorized to receive it.
   c. There is evidence of break-in to an office or locked file cabinet.
   d. There is evidence of someone trying to hack into a computer or network.

   e. There is evidence, through media story or other source, which indicates that CDCPB staff intentionally or unintentionally released CDCPB confidential information that is out of compliance with CDCPB S&C.
2. If a breach occurs, notify the Section Supervisor immediately.
   a. If the Section Supervisor is not available, notify the CDCPB Bureau Chief.
   b. The Section Supervisor will notify staff or other persons as appropriate.
   c. Refer all media inquiries to the Section Supervisor.
3. Investigate any breach of confidentiality immediately to determine cause(s), mitigate immediate outcomes, and prevent future breaches.
4. Notify program contacts.
   a. The Section Supervisor promptly notifies the appropriate representative for a CDC-sponsored or other federal program.
5. Determine whether to notify legal contacts.
   a. The ORP, Section Supervisor, and CDCPB Chief determine:
      i. whether to notify DPHHS legal counsel, and
      ii. in conjunction with legal counsel, whether to notify law enforcement agencies.
6. A violation of CDCPB S&C can result in disciplinary action, termination of employment, loss of professional licensure, and/or legal prosecution.

IV. DEFINITIONS

Authorized user (or Authorized personnel): person who is authorized by the ORP and completes required training for accessing CDCPB confidential information for a justifiable public health use. This may include: CDCPB staff, DPHHS TSD staff, DPHHS non-CDCPB staff, and non-DPHHS users.

Breach: a departure from established policies or procedures or a compromise, unauthorized acquisition, unauthorized access, or loss of control of personally identifiable information.

Confidential information: any private information about an identifiable person who has not given consent to make the information public.

DPHHS TSD staff: DPHHS staff who is employed by the DPHHS Technology Services Division.

Encryption: manipulation or encoding of information so that only parties intended to view the information can do so.

Facility list: a line list of cases reported by a particular facility or care provider that is distributed to that facility for its records.

Form: the instrument used by the CDCPB to record case information provided by a health professional or abstracted from medical records.

CDCPB staff: DPHHS staff who is employed in the Communicable Disease Control and Prevention Bureau.

HIV/AIDS-related information: terms, variable names, or statements that, if appearing on a form or other document, could identify an individual as having HIV or AIDS. Examples include: CD4 lab test results, HIV Western blot, HIV viral load, and the terms “HIV” or “AIDS.”

Line list: any list of names of cases or patients, generated from any source that is used for disease surveillance purposes.

Overall Responsible Party (ORP): the state employee with ultimate responsibility for updating and maintaining the confidentiality policy of the CDCPB and ensuring it is met.

Personal identifier: information that allows the identity of a person to be determined with a specified degree of certainty. This could be a single piece of information or several pieces of data which, when taken together, may be used to identify an individual.

Potentially identifying information: information, which when combined with other information, could potentially identify and/or cause harm to an individual or individuals. This includes but is not limited to such information as medical record/case numbers, and demographic or locality information that describes a small subset of individuals (e.g. block data, zip codes, some race/ethnicity data).

Protected health information: individually identifiable health information, which can be linked to a particular person. Specifically, this information can relate to: the individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or, the past, present, or future payment for the provision of health care to the individual. Common identifiers of health information include names, social security numbers, addresses, and birth dates.

Record: the permanent file kept on an individual case. It includes all original case report forms, laboratory reports, the death certificate, and any other information relevant to that case. Records are kept in the central office only and never in regional offices.

Secure container: a bag, case, or satchel that can be fastened shut and that can carry all surveillance information necessary for field activities.

Security: protection of public health data and information systems to prevent unauthorized release of identifying information and accidental loss of data or damage to the systems.

Surveillance information: all information used or collected for surveillance activities, including that contained in line lists, case report forms, laboratory reports, computer files, and correspondence relating to individual cases.

V. REFERENCES AND RELATED MATERIALS

A. Centers for Disease Control and Prevention. *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action*. Atlanta (GA): U.S. Department of Health and Human Service, Centers for Disease Control and Prevention; 2011. http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf

B. Montana Department of Public Health and Human Services (DPHHS) Health Insurance Portability and Accountability Act (HIPAA) training (http://ours.hhs.mt.gov/hipaa/hipaatraining.pdf

C. State of Montana's Office of Epidemiology and Scientific Support. *Guidelines for the Release of Public Health Data Derived from Personal Health Information*. https://dphhs.mt.gov/Portals/85/publichealth/documents/Epidemiology/GuidelinesReportingPHI.pdf

D. Summary of HIPAA Privacy Rule
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

VI. ATTACHMENTS

A. Appendix A: Resignation/Termination Checklist (Parts 1 & 2)
B. Appendix B: CDCPB S&C Training Checklist
C. Appendix C: Request for Personal Health Information
D. Appendix D: Recommendations for Maintaining Confidentiality for Reporting Providers
E. Appendix E: Guidelines for the Use of Facsimile Machines
F. Appendix F: Sample Confidentiality Disclaimer

VII. LEGAL REFERENCES

The Confidentiality of Health Care Information statute (MCA 50-16-603) and the Permissible Release of Information Concerning Infected Persons statute (MCA 50-18-109) describe the allowable disclosure of confidential health care information in carrying out public health activities. This security and confidentiality policy and procedures manual is aligned with these statutes.

Title 50. Health and Safety, Chapter 16. Health Care Information, Part 6. Government Health Care Information; http://leg.mt.gov/bills/mca/50/16/50-16-603.htm
50-16-603. Confidentiality of health care information.

Health care information in the possession of the department, a local board, a local health officer, or the entity's authorized representatives may not be released except:

(1) for statistical purposes, if no identification of individuals can be made from the information released;

(2) when the health care information pertains to a person who has given written consent to the release and has specified the type of information to be released and the person or entity to whom it may be released;

(3) to medical personnel in a medical emergency as necessary to protect the health, life, or well-being of the named person;

(4) as allowed by Title 50, chapters 17 and 18;

(5) to another state or local public health agency, including those in other states, whenever necessary to continue health services to the named person or to undertake public health efforts to prevent or interrupt the transmission of a communicable disease or to alleviate and prevent injury caused by the release of biological, chemical, or radiological agents capable of causing imminent disability, death, or infection;

(6) in the case of a minor, as required by 41-3-201 or pursuant to an investigation under 41-3-202 or if the health care information is to be presented as evidence in a court proceeding involving child abuse pursuant to Title 41, chapter 3. Documents containing the information must be sealed by the court upon conclusion of the proceedings.

(7) to medical personnel, the department, a local health officer or board, or a district court when necessary to implement or enforce state statutes or state or local health rules

concerning the prevention or control of diseases designated as reportable pursuant to 50-1-202, if the release does not conflict with any other provision contained in this part.

History: En. Sec. 3, Ch. 481, L. 1989; amd. Sec. 10, Ch. 391, L. 2003; amd. Sec. 26, Ch. 504, L. 2003.

Title 50. Health and Safety, Chapter 18. Sexually Transmitted Diseases, Part 1. General Provisions; http://leg.mt.gov/bills/mca/50/18/50-18-109.htm

50-18-109. Permissible release of information concerning infected persons.

(1) Information concerning persons infected or reasonably suspected to be infected with a sexually transmitted disease may be released only:

(a) to personnel of the department of public health and human services;

(b) to a physician who has written consent of the person whose record is requested;

(c) to a local health officer; or

(d) by the department of public health and human services or a local health officer or board under the circumstances allowed by Title 50, chapter 16, part 6.

(2) For the purposes of this section, the term "information" includes all knowledge or intelligence and all communications of all knowledge or intelligence, oral or written or in record form, and also includes but is not limited to information concerning the location or nature of the activities or work of all local, state, or federal employees or officers engaged in sexually transmitted disease eradication work. Communications to and from personnel are privileged as provided in 26-1-810.

(3) The purpose of this section is to protect and preserve the principle of confidentiality in sexually transmitted disease work by local, state, and federal public personnel, as confidentiality is important to the success of all sexually transmitted disease eradication work and endeavor, and to require that the principle of confidentiality in the work remain inviolate.

History: En. Sec. 106, Ch. 197, L. 1967; amd. Sec. 1, Ch. 135, L. 1971; amd. Sec. 109, Ch. 349, L. 1974; R.C.M. 1947, 69-4610; amd. Sec. 8, Ch. 440, L. 1989; amd. Sec. 117, Ch. 418, L. 1995; amd. Sec. 294, Ch. 546, L. 1995.

VIII. POLICY HISTORY

A. Original entitled: Montana HIV/AIDS Surveillance Program, Security and Confidentiality Policy, December 26, 2012 [in compliance with CDC Revision of *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action*]

A. Revised: Entitled Communicable Disease Control and Prevention Bureau Security and Confidentiality Policy (CDCPB S&C): October 15, 2014

B. Revised: October 15, 2018

II. APPENDICES

Appendix A: Resignation/Termination Checklist (Parts 1 & 2)

Resignation/Termination Checklist Part 1

Employee Name: _____

☐ Reviewed confidentiality issues with employee

☐ File cabinets and office secured

☐ Keys to office building, person office, and file cabinets surrendered to: _____

☐ State identification turned in

☐ Voice mail cleared on personal telephone. Voice mail passcode: _____

☐ Email cleared on computer. Email passcode: _____

☐ All equipment turned in

☐ Computer passwords changed.

☐ Encryption anywhere password: _____ Screen saver password: _____

☐ All files in the employee's personal folders on the H: drive have been moved or deleted

☐ Final time sheet received. Final paycheck to be sent to:

_____

Signature of Supervisor Date

I hereby certify that all keys to secured areas and identification badges have been returned, and that no paperwork, diskettes, or other media containing confidential information remain is in my possession. I understand that all patient information is to remain confidential. I understand that persons who reveal confidential information may be subject to legal action by the person about whom such information pertains.

_____

Signature of Employee Date

Appendix A: Resignation/Termination Checklist (Parts 1 & 2) cont.

Resignation/Termination Checklist Part 2

Date: _____

(To be completed by supervisor or designee immediately following employee departure)

☐ Email sent to Computer Technician to cancel email account

☐ Federal project staff notified (if applicable). Name of person notified: _____

☐ CDC Secure Network account cancelled (if applicable)

☐ All staff notified by email of departure

_____

Signature of Supervisor Date

Appendix B: CDCPB S&C Training Checklist

Montana Communicable Disease Control and Prevention Bureau Confidentiality Checklist

As a Communicable Disease Control and Prevention Bureau (CDCPB) employee, subcontracted employee, student, visiting professional, or Technology Services Division (TSD) staff, 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 by various governmental regulations.

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 Confidentiality Policy readily available.
- I understand that I am bound by these policies, even upon resignation, termination, or completion of my activities.

2. Offices Initials _____

- Confidential information, keys and/or passwords are secured in my office when it is not occupied.
- 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 secure 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 confidential information may be utilized. I ensure that the visitor, whether client or outside professional, is brought to a private area before beginning any conversation in which confidential patient information is discussed.
- 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.

3. Mail Initials _____

- I am aware that mail addressed to a specific CDCPB 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).
- When mailing hardcopies with identifiers, I send no more than 100 names/identifiers per envelope.
- I confirm receipt of any confidential package I send.

4. Telephone/Fax/Email Initials _____

- I never send information that contains confidential personal identifiers by email (even with encryption). I do not email medical record numbers.
- 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 where the conversation will not be overheard.
- I never leave personal identifiers related to confidential records on non-confidential voicemail messages.

5. Handling of Paper Records Initials _____

- When not in use, I store all documents with confidential information in a locked filing/storage cabinet within a secured area.
- 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 when possible, I transport confidential information coded to disguise any term that could easily be associated with a specific disease.
- Confidential records may <u>not</u> be taken home or to a motel 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, 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.
- If necessary, I always clear the copier by making a single blank copy following the

duplication of any confidential information.

- 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.

6. 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 always situated so that they are not visible to unauthorized personnel or through ground level windows. If needed, I use a privacy screen.
- I understand that I am responsible for maintaining the virus definitions and other updates to my laptop (Field staff are also responsible for this maintenance for desktop computers).
- Unless required by travel, I always store my laptop in a secure, locked location in the office when not in use. 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 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.

7. 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 encrypted using PGP 3072-bit encryption (or other 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 PGP 3072-bit encryption (or other approved encryption); 3) are stored in a locked container when not in use; 4) are never taken into the field without appropriate encryption; and 5) are electronically wiped following completion of the task.
- I electronically transfer sensitive data only if it is encrypted using PGP 3072-bit encryption (or other approved encryption).

8. 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 Confidentiality Policy.
- If I am responsible for preparing and/or releasing reports/statistics, I fully understand all of the procedures outlined in Sections IX and X of the Confidentiality Policy and I always obtain the appropriate releases and Confidentiality Agreements, as specified in the Confidentiality 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 Confidentiality Policy and I always obtain the appropriate releases and confidentiality agreements as specified in the Confidentiality 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.

<u>Warning:</u> 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 Communicable Disease Control and Prevention Security and Confidentiality Policy. I have received, read, understand, and agree to comply with the guidelines.

_____

Signature of Employee Date

_____

Signature of Supervisor Date

Appendix C: Request for Personal Health Information

Request for Personal Health Information

Under the Health Insurance Portability and Accountability Act (HIPAA), you have the right to access your personal health information ("PHI") that is held by the Department of Public Health and Human Services (DPHHS). There are some exceptions, but DPHHS will accommodate all reasonable requests. This form allows you to request specific PHI pertaining to you.

Name: _____ Date of birth: _____

Social Security Number: _____

I authorize the Department of Public Health and Human Services to release the following PHI to me:

☐ All information

☐ Information from a specific time period (specify dates): from _____ to _____

☐ All information relating to a specific event or condition (specify event and time period)

Event: _____

Date(s) of event: from _____ to _____

☐ Other (please specify): _____

_____

_____

_____

Signature: _____ Date: _____

Address: _____ City: _____ State: _____ Zip: _____

Phone: _____

Appendix D: Recommendations for Maintaining Confidentiality for Reporting Providers

RECOMMENDATIONS FOR MAINTAINING CONFIDENTIALITY FOR REPORTING PROVIDERS

As health care professionals, it is important that we take great care in guarding the health status of patients. It is particularly important that we protect the confidentiality of HIV/AIDS patients, since persons with HIV/AIDS may be subject to discrimination. Listed below are just a few of the recommendations from the Centers for Disease Control and Prevention (CDC) for maintaining the confidentiality of persons diagnosed with HIV.

1) Whenever possible, remove any information from the outside of charts and patient lists that may automatically identify an individual as being HIV positive to those not directly involved in the patient's care.
2) Never leave information that discloses a patient's HIV status (e.g., lab reports, medical records, insurance claims) where others not directly involved in the patient's care might easily read it.
3) Never discuss a patient's HIV status within earshot of other patients or non-health care individuals.
4) When reporting a positive case to the Office of Public Health, be sure to speak with one of the surveillance epidemiologists or to the HIV/AIDS Surveillance Program Manager listed below.
5) Please do not leave any identifying information about a patient on voice mail. Leave your name and number and your call will be promptly returned.
6) Please mail all information concerning HIV/AIDS patients in double envelopes and mark the inside envelope as "confidential." This helps protect the confidentiality of patients if an unauthorized person opens the mail or the outer envelope is accidentally ripped.

Following these simple guidelines will help decrease the risk of accidental disclosure of a patient's status. If you have any other questions or concerns about confidentiality, please feel free to contact Helen McCaffrey, the HIV/AIDS Surveillance Epidemiologist (406-444-4735; hmccaffrey@mt.gov).

Appendix E: Guidelines for the Use of Facsimile Machines

Guidelines for the Use of Facsimile Machines*

(From The Centers for Disease Control and Prevention. Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action. Atlanta (GA): U.S. Department of Health and Human Services, Centers for Disease Control and Prevention; 2011)

Although facsimile (fax) equipment and software can enhance the quality of health care by facilitating rapid transmission of health information, this same mode of transmission opens up the possibility that information will be misdirected or intercepted by persons for whom access is not intended or authorized. In recent years, numerous reports have described events wherein patient health records were inadvertently faxed to a wrong location (e.g., bank or retail store) rather than the intended recipient. The following recommendations will help minimize the risks associated with use of facsimile machines.

- Establish fax policies and procedures based on federal guidelines, state laws and regulations, and consultation with legal counsel, as needed.
- Take reasonable steps to ensure that the fax transmission is sent to the intended destination. As possible, pre-program and periodically audit and test destination numbers to eliminate errors in transmission from misdialing and outdated fax numbers. Periodically, remind frequent recipients of PII to notify the program of any changes in fax number. Train staff to double check the recipient's fax number before pressing the 'send' key.
- Provide education and training to staff on the program's fax policies and procedures. This includes educating private providers and laboratories that report information to public health programs. Take reasonable operational safeguards to alert staff of faxing procedures. For example, affix brightly colored stickers to fax machines reminding staff of key fax policies (e.g., need for a cover sheet; verification of recipient's fax number; and procedures to implement if an incoming fax has been received in error).
- Require all fax communications be sent with a cover sheet that includes name and contact information of the sender and the recipient, confidentiality disclaimer statement, and instructions on what to do if the document is received in error (see Sample Confidentiality Disclaimer below).
- If a fax transmission fails to reach the recipient, check the internal logging system of the fax machine to obtain the number to which the transmission was sent. If the sender becomes aware that a fax was misdirected, contact the receiver and ask that the material be returned or destroyed. Investigate misdirected faxes as a risk management occurrence or security incident, inform the ORP, and log the incident for remediation/mitigation.
- Locate fax machines in secure areas.
- Ensure that data security policies include procedures for maintaining and disposing of paper fax transmissions.

** Based on "Facsimile Transmission of Health Information"*

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031811.hcsp?dDocName=bok1_031811

Appendix F: Sample Confidentiality Disclaimer

Sample Confidentiality Disclaimer

The documents accompanying this fax transmission contain health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.