Montana Department of Public Health and Human Services
Laboratory Services Bureau

Biosecurity Plan

B. Security of Data and Electronic Technology Systems

MTPHL's electronic laboratory information is secured by various mechanisms.

- The MTPHL uses operating systems installed and secured by the State of Montana Information Technology and Services Division (ITSD), and network access is password protected. Passwords must be reset on a regular basis and conform to state standards. All computers have virus scanning software, and e-mail downloads of executable files or other files of risk are prohibited. There is a strict internet browsing policy, and certain sites are blocked from access. These blocks are tracked, and employees surfing to an unusual number of blocked websites is reported by ITSD to management. The State of Montana has secure firewalls, and network drives are backed up daily. Information Technology specialists assess the security of the hardware and software products in addition to the security of local area networks.
- Laboratory Information Management Systems used by MTLSB are password protected.
- MTPHL Data Coordinators and System Administrators for the LIS have the authority to set security limits for each individual user in of the LIS. Each user is assigned to a security group, or role, depending on their work-related tasks.
- Hard copies of electronic records are maintained and stored as a backup security measure for electronic storage of documents, including a hard copy of the Select Agent Inventory Form. These documents are stored in a locked cabinet, known to the RO and ARO(s) for a minimum of three (3) years.
- Paper data is stored in filing cabinets or boxes in the various sections of the LSB behind key card access doors, or in locked storage rooms. Paperwork not related to Select Agents will be maintained for a minimum of two (2) years; Select Agent paperwork will be maintained for a minimum of three (3) years. Sensitive Select Agent paperwork is stored in the BSL-3 area where there is the highest level of security.
- Laboratory personnel are expected to maintain confidentiality of all sensitive information, be it verbal, paper or electronic. This includes computer screen displays, specimen requisition forms, or face-to-face discussions. After a period of inactivity, the computer automatically locks, and a password is needed to unlock the workstation. If the employee resides outside of the locked doors in areas accessible by the public, they are requested to lock their computer prior to leaving the computer unattended.

Please Note: The entire MTPHL Biosecurity Plan cannot be shared publicly due to the Select Agent Program Regulations. If you have additional questions, please contact MTPHL directly: 1-800-821-7284