

641—154.54(124E) Security requirements.

154.54(1) Security policy requirement. A laboratory shall maintain a security policy to prevent the loss, theft, or diversion of medical cannabidiol samples. The security policy shall apply to all staff and visitors at a laboratory facility.

154.54(2) Restricted access. A laboratory shall limit entrance to all restricted areas by completing all of the following:

a. The controlled access system shall do all of the following:

- (1) Limit access to authorized individuals;
- (2) Maintain a log of individuals with approved access, including dates of approvals and revocations;
- (3) Track when personnel enter and exit the laboratory;
- (4) Track times of personnel movement between restricted access areas;
- (5) Store data for retrieval for a minimum of one year; and
- (6) Remain operable in the event of a power failure.

b. A laboratory shall promptly, but no later than five business days after receipt of request, submit stored controlled access system data to the department.

154.54(3) Personnel identification system. A laboratory shall use a personnel identification system that controls and monitors individual employee access to restricted access areas within the laboratory facility.

a. An employee identification card shall contain:

- (1) The name of the employee;
- (2) The date of issuance and expiration;
- (3) An alphanumeric identification number that is unique to the employee; and
- (4) A photographic image of the employee.

b. A laboratory employee shall keep the identification card visible at all times when the employee is in the laboratory.

c. Upon termination or resignation of an employee, a laboratory shall immediately:

- (1) Revoke the employee's access to the laboratory; and
- (2) Obtain and destroy the employee's identification card, if possible.

154.54(4) Video monitoring and surveillance. A laboratory shall operate and maintain in good working order a video surveillance system for its premises that operates 24 hours per day, seven days a week, and visually records all areas where medical cannabis goods are stored or tested.

a. *Camera specifications.* Cameras shall:

- (1) Capture clear and certain identification of any person entering or exiting a restricted access area containing medical cannabis goods;
- (2) Produce a clear, color still photograph live or from a recording;
- (3) Have an embedded date-and-time stamp that is synchronized to the recording and does not obscure the picture; and
- (4) Continue to operate during a power outage.

b. *Video recording specifications.* Video recording equipment shall:

- (1) Export still images in an industry standard image format, such as .jpg, .bmp, or .gif.
- (2) Archive in a format that ensures authentication and guarantees that the recorded image has not been altered.

(3) Save exported video in an industry standard file format that can be played on a standard computer operating system.

(4) All recordings shall be erased or destroyed at the end of the retention period and prior to disposal of any storage medium.

c. *Additional requirements.* A laboratory shall maintain all security system equipment and recordings in a secure location to prevent theft, loss, destruction, corruption, and alterations.

d. *Retention.* A laboratory shall ensure that 24-hour recordings from all video cameras are:

- (1) Available for viewing by the department upon request;
- (2) Retained for a minimum of 60 days;
- (3) Maintained free of alteration or corruption; and

(4) Retained longer, as needed, if a laboratory is given actual notice of a pending criminal, civil, or administrative investigation, or other legal proceeding for which the recording may contain relevant information.

154.54(5) *Chain-of-custody policy and procedures.* A laboratory shall maintain a current chain-of-custody policy and procedures. The policy should ensure that:

a. Chain of custody is maintained for samples that may have probable forensic evidentiary value; and
b. Annual training is available for individuals who will be involved with testing medical cannabis goods.

154.54(6) *Information technology systems security.* A laboratory shall maintain information technology systems protection by employing comprehensive security controls that include security firewall protection, antivirus protection, network and desktop password protection, and security patch management procedures.

[ARC 8124C, IAB 7/10/24, effective 8/14/24]