

# Security Plan and Manual

State of Maryland  
Maryland Department of Health  
Laboratories Administration

1770 Ashland Avenue  
Baltimore, Maryland 21205

Manual issued to:

**April 1, 2020**

Version 2.2




**State of Maryland**  
**Maryland Department of Health**  
**Laboratories Administration**  
**Central Lab**  
**Review/Approve of Document**

The Laboratories Administration Central Lab's "**Security Plan and Manual**" has been reviewed and approved for use in the MDH Laboratories Administration Central Lab located at 1770 Ashland Ave. facility, effective 4/1/2020.  
*Date effective*

  
\_\_\_\_\_  
**Rachel V. Michael**  
**Safety and Security Officer**

4/17/2020  
\_\_\_\_\_  
**Date approved**

  
\_\_\_\_\_  
**Robert A. Myers, Ph.D.**  
**Director, Laboratories Administration**

04/22/2020  
\_\_\_\_\_  
**Date approved**



## Annual Review of Laboratories Administration Security Plan and Manual

The Laboratories Administration *Security Plan and Manual* will be reviewed on an annual basis. This review may take the form of a Drill or Exercise, a Table-Top Exercise, an After-Action Report/Review of an actual event, or a Document Review of the *Security Plan and Manual*. The annual review is a requirement to verify the Plan's effectiveness, and will be documented using this form.

---

This review is a (n) (check all that apply):

**Drill/Exercise**

List all parties participating and the scenario used for the exercise. Include any pertinent problems or questions that arise. Attach additional documentation to this sheet.

**Table-Top Exercise**

List all parties participating and the scenario used for the exercise. Include any pertinent problems or questions that arise. Attach additional documentation to this sheet.

**Document Review of the *Security Plan and Manual***

A Document Review states the *Security Plan and Manual* have undergone a thorough evaluation, and does not require any additional modifications or further review at this time. No additional attachments are needed.

**After-Action Report/Review of an Actual Event**

If an event requiring the implementation of the *Security Plan and Manual* takes place, the event may be substituted for a Document Review and/or a Table Top Exercise. Attach additional documentation providing a summary of the event, and a full explanation as to how the *Security Plan and Manual* was employed, as well as any problems that arose pertaining to the Plan.

Review Conducted By: Rachel V. Michael  
Safety & Security Officer

Date: 4/17/2020

Review Conducted By: Robert A. My  
Laboratories Administration Director

Date: 04/20/2020



## Revision History

### Security Plan and Manual

REVISION	COMMENTS	DATE
Original	After 9/11/2001 DHMH Laboratories Administration established a written Security Plan and Manual. The Security Plan and Manual for the 1770 Ashland Avenue facility has been prepared with the intent to reflect the relevant content of original manual, incorporate updated information and ensure compliance with the <i>Public Health Security and Bioterrorism Preparedness and Response Act of 2002</i> and 7 CFR Part 331, 9 CFR Part 121, and 42 CFR Part 73.	5/1/2015
Version 1.1	The Security Plan and Manual has been updated to include additional information regarding workplace violence, package and shipping, and employee temporary keycards.	5/3/2016
Version 1.2	The Security Plan and Manual have been updated to include revisions to contact information.	4/1/2017
Version 2.0	The Security Plan and Manual has been revised to reflect the name change of the Department of Health & Mental Hygiene to Maryland Department of Health. Additionally, the visitor authorization requirements have been revised and updated. The following appendices were updated “1770 ID Request Form” Appendix B, SOP for Requesting Health Records Appendix G, “Request to Access Health Records Form” new Appendix H and “Revocation of Access to Records Form” new Appendix I.	6/1/2017 7/1/2017 3/12/2018
Version 2.1	The Security Plan and Manual have been revised and updated to include a new procedure on how to handle a “Suspicious Package,” as well as a new procedure and form for employee separation “MDH Employee Offboarding Supervisor’s Checklist”.	11/19/2018 3/12/2019
Version 2.2	The Security Plan and Manual has been revised and updated to include changes to the Cyber Security sections and to reflect the facility management name change from Forest City to Brookfield Properties.	4/13/2020





# EMERGENCY NUMBERS

**Lobby Security Desk.....443-681-3795**

**Loading Security Desk.....443-681-3808**

**Safety & Security Officer.....443-681-3792**

**Security Emergency..... 3911**

**\*\*For life threatening emergencies dial 911\*\***

## PREFACE

This *Security Plan and Manual* brings together information that will assist both you and your supervisors to meet security responsibilities through a formal security program. This program encompasses a broad range of requirements and responsibilities designed to protect the safety of employees, visitors, and the surrounding community by securely maintaining a work site that routinely possesses, works with, and transfers hazardous biologic agents, hazardous chemicals, and sources of hazardous radiation.

The success of our security program depends on upon you having the necessary knowledge to carry out the program. When you are aware of risks you are less likely to breach security. Everyone who works at a site containing hazardous materials should have this knowledge. It includes knowing how to protect yourself and your co-workers. It also includes knowing how to respond to a range of security emergencies including, a breach of patient confidentiality, the loss of a laboratory key, the observed breakdown in controlled access to a toxic agent, the removal of an individual who is not authorized to be in a laboratory, etc.

The degree of safe, secure practices (operational security) observed in a laboratory stems directly from the attitudes and actions of the people in charge. The responsibility for enforcing our security program ultimately rests with the Laboratory Director. However, immediate responsibility rests with every supervisor, employee, and our uniformed police officers.

Supervisors must ensure that each member of their staff understands the applicable contents of this security manual. Supervisors must also oversee and demand observance of the policies in this manual. Supervisors must educate themselves as fully as possible about security risks and relay this information to their employees.

Remember, you are the only person who can truly practice operational security for your own protection and that of your fellow workers. Therefore, you are required to know, understand, and adhere to the policies of this security manual.

This *Security Plan and Manual* has been reviewed and approved for distribution to MDH Laboratories Administration employees and agencies whose employees have been granted access to the Central Lab at 1770 Ashland Avenue, Baltimore, Maryland 21205.



# Table of Contents

<b>I. Information Security</b> .....	7
A) Patient Medical Information and Records .....	7
<b>B) Access to Patient Medical Laboratory Records</b> .....	7
<b>C) Non-Medical Laboratory Confidential and Sensitive Information and Records</b> .....	8
<b>D) Access to Confidential or Sensitive Non-Medical Laboratory Records</b> .....	9
<b>E) Disposition of Confidential and Sensitive Records</b> .....	9
<b>F) Cybersecurity</b> .....	10
<b>A) The LA is required to comply with all MDH and DoIT security policies intended to assure the security, confidentiality, and integrity of electronic information as set forth in the following MDH policies: <a href="https://health.maryland.gov/oit/doc/DHMH_IT_SecurityPolicy2014%20(1).pdf">https://health.maryland.gov/oit/doc/DHMH_IT_SecurityPolicy2014%20(1).pdf</a> and DoIT Security Policy: <a href="https://doit.maryland.gov/Publications/State_of_Maryland_ITMP_FY19.pdf">https://doit.maryland.gov/Publications/State_of_Maryland_ITMP_FY19.pdf</a></b> .....	10
<b>B) LA Information Technology (IT) Infrastructure and Security</b> .....	10
<b>II. Physical Security</b> .....	12
A) Access to Maryland Department of Health, J. Mehsen Joseph Public Health Laboratories Administration, Central Lab, 1770 Ashland Ave., Baltimore, MD 21205 .....	12
B) When Building Access May be Obtained .....	13
C) Emergency Evacuation .....	13
D) Suspicious Package.....	14
E) Active Shooter/Assailant Awareness .....	15
F) Security Barriers, Video Surveillance System, and Access Control Database .....	16
G) Access to Biological Select Agent and Toxin (BSAT) Work and Storage Areas.....	17
H) Waste Storage and Removal .....	21
I) Packaging and Shipping Dangerous Goods.....	22
J) Role of Safety and Security Officer .....	22
K) Brookfield Properties Security Officers Posted at 1770 .....	22
L) Brookfield Properties Security Enforcement of Security Plan .....	23
M) Brookfield Properties Security Officer- LA Employee Interactions .....	24
N) LA Key Contacts.....	25
O) Brookfield Properties Building and Security Key Contacts .....	26
P) Brookfield Properties Security Roles and Responsibilities.....	26

Q) Metal Keys and Locks.....	27
R) 1770 Photo ID Keycard.....	28
S) Policy and Procedure for LA Employee without a government issued photo identification needing a TEMP keycard.....	31
T) Maryland State ID .....	31
U) State Property Passes.....	33
<b>III. Security Policies.....</b>	<b>33</b>
A) Visitors in the Workplace Policy.....	34
B) Security Awareness .....	35
<b>IV. Appendix A Laserfiche Visitor Clearance Sheet .....</b>	<b>37</b>
<b>V. Appendix B 1770 ID Request, Separation, and Security Access Form.....</b>	<b>38</b>
<b>VI. Appendix C 1770 Security Incident/Breach Reporting Form .....</b>	<b>39</b>
<b>VII. Appendix D Locker Request Form .....</b>	<b>40</b>
<b>VIII. Appendix E MDH 1770 Building Key Request Metal Keys.....</b>	<b>41</b>
<b>IX. Appendix F MDH Employee Offboarding Supervisor’s Checklist.....</b>	<b>42</b>
<b>X. Appendix G <i>Standard Operating Procedure for Requests for Protected Health Information</i> .....</b>	<b>43</b>
<b>XI. Appendix H <i>Request for Protected Health Records Form</i> .....</b>	<b>47</b>
<b>XII. Appendix I <i>Revocation of Access to Records Form</i>.....</b>	<b>49</b>
<b>XIII. Appendix J <i>Records Retention and Disposal Schedule</i> .....</b>	<b>50</b>
<b>XIV. Appendix K <i>1770 Tenant Handbook</i>.....</b>	<b>51</b>
<b>XV. Appendix L Laboratories Administration Employee Temporary Keycard Authorization Form.....</b>	<b>52</b>

## **I. Information Security**

### **A) Patient Medical Information and Records**

Laboratories Administration (LA) is responsible for maintaining the confidentiality of patient information and records against all types of unauthorized use.

#### a) Confidential information and records:

- (1) Includes any and all types of information (oral, written or electronic) that identifies, or can be traced back to a patient or client;
- (2) May include requisition forms, worksheets, report forms, telephone logs, electronic databases, bills, etc.

#### b) Responsibility for protecting confidential information and records:

- (1) Every LA employee who comes in contact with confidential information and/or records is responsible for maintaining that confidentiality;
- (2) Failure to maintain patient/client confidentiality will subject employee(s) to disciplinary action, up to and including immediate dismissal from State service.

#### c) Maintain confidentiality by ensuring all confidential information and records are:

- (1) Discussed only within the work area;
- (2) Formally or informally relayed only to an authorized third party;
- (3) Not visible in rooms accessible to the public;
- (4) Not left sitting open or visible while awaiting photocopying;
- (5) Mailed in sealed envelopes; and
- (6) Discarded following proper procedures [See Section I. E.].

### **B) Access to Patient Medical Laboratory Records**

#### **A) Access by Patients:**

- (1) A laboratory record is the property of the LA and MDH; however, the patient has a right to information in the record.
- (2) The LA may not deny a patient (or his/her authorized representative) access to information in the record when the patient places a written request for the information, and the

laboratory has informed the patient's physician that information is being released. (See Laboratories Administration "*Standard Operating Procedure for Requests for Protected Health Information*" Appendix G, "Request to Access to Records Form" Appendix H, and/or "Revocation of Access to Records Form Appendix I or contact the Deputy Director for Administrative and Support Operations,).

- (3) Regarding Telephone, Email, and Faxed requests. (See Laboratories Administration "*Standard Operating Procedure for Requests for Protected Health Information*" or contact the Deputy Director for Administrative and Support Operations, Appendix G).

**B) Access by Third Parties:**

- (1) Medical laboratory records may be released by written request or according to the provisions of a court-ordered subpoena. (See Laboratories Administration "*Standard Operating Procedure for Requests for Protected Health Information*" or contact the Deputy Director for Administrative and Support Operations, Appendix G).

**C) Non-Medical Laboratory Confidential and Sensitive Information and Records**

LA is responsible for maintaining the confidentiality of client and Administration non-medical lab-related information and records against all types of unauthorized use.

**A) Confidential information and records:**

- a) Includes any and all types of information [oral, written, electronic, any paper, correspondence, form, photograph, recording, microfilm, magnetic tape, diskette, compact disk (CD), digital video disc (DVD) file, table, chart, map, drawing, database, email, document regardless of physical or characteristics] that may potentially involve litigation, personal knowledge, attorney-client privileged information, certain scientific or technical information, certain business information, etc.
- b) May include requisition forms, worksheets, report forms, telephone logs, electronic databases, bills, social security numbers, grievance materials, disciplinary documentation, PEP evaluations, non-winning award nominations, Standard Operating Procedures Manual (SOPM), lists involving select agents, etc.

**B) Protecting non-medical confidential and sensitive information and records:**

- a) Every employee who comes into contact with confidential or sensitive information or records is responsible for maintaining that confidentiality;
- b) Failure to maintain this confidentiality will subject an employee to disciplinary action, up to and including immediate dismissal from State service.

**C) Maintain confidentiality by ensuring all confidential information and records are:**

- a) Discussed only inside the work area;
- b) Formally or informally relayed only to an authorized third party;
- c) Not left open on desks or lab benches in unlocked space;
- d) Not left sitting open while awaiting photocopying;
- e) Mailed in sealed envelopes; and
- f) Discarded only following proper procedures [See Section I. E.]

**D) Access to Confidential or Sensitive Non-Medical Laboratory Records**

- A)** Confidential or Sensitive Non-Medical Laboratory Records may be released to authorized third party:
  - a) Under a court-ordered subpoena after informing and consulting the Division/Regional Lab Chief and Director;
  - b) If public records, under Maryland’s Public Information Act; and
  - c) To State auditors or other Departmental agencies authorized under various State laws and regulations to access them.

**E) Disposition of Confidential and Sensitive Records**

**A) Retention Requirements**

- a) The retention of official records will conform to the schedule detailed in the approved MDH Laboratories Administration’s *Records Retention and Disposal Schedule*. (Department of General Services –State Records Center Schedule Number 2582, pg. 1-20, “DHMH Laboratories Administration This Schedule Supersedes Schedule 220.” Appendix J)
- b) MDH Laboratories Administration’s policies and procedures will be followed when records are to be destroyed per the approved schedule. Disposition can only be performed by individuals who have received documented training in records management (Refer to “Laboratories Administration Records Management Standard Operating Procedure,” SOP 9/16/2013.)

**B) Authorization to Dispose of Confidential and Sensitive Records**

- a) Employees must always consult a supervisor before disposing of routine medical laboratory records or business records;



- b) Employees must always consult with the Division Chief or Director before disposing of non-routine medical laboratory records, forensic/legal records, and auditable business records.

**C) Disposal Methods**

- a) The disposal of records, any confidential or sensitive record, must follow the current DHMH Laboratories Administration's *Records and Disposal Schedule* and "Laboratories Administration Records Management Standard Operation Procedure." ( Refer to "Department of General Services –State Records Center Schedule Number 2582, pg. 1-20, "DHMH Laboratories Administration This Schedule Supersedes Schedule 220" Appendix J, and "Laboratories Administration Records Management Standard Operating Procedure," SOP 9/16/2013.)
- b) Non-Record Material, temporary materials, including but not limited to meeting agendas, calendars, reference materials, stock publications, speech notes, information letters, draft SOPs, obsolete equipment manuals, and procedures, may be recycled.

**F) Cybersecurity**

- A) The LA is required to comply with all MDH and DoIT security policies intended to assure the security, confidentiality, and integrity of electronic information as set forth in the following MDH policies: [https://health.maryland.gov/oit/doc/DHMH\\_IT\\_SecurityPolicy2014%20\(1\).pdf](https://health.maryland.gov/oit/doc/DHMH_IT_SecurityPolicy2014%20(1).pdf) and DoIT Security Policy: [https://doit.maryland.gov/Publications/State\\_of\\_Maryland\\_ITMP\\_FY19.pdf](https://doit.maryland.gov/Publications/State_of_Maryland_ITMP_FY19.pdf)**

- a) MDH Policy 02.01.01 DHMH Information Technology Security Policy;
- b) MDH Policy 02.01.02 Software Copyright Policy & the State of Maryland Software Code Of Ethics;
- c) MDH Policy 02.01.03, The Acquisition & Utilization Of Information Technology Resources; and
- d) MDH Policy 02.01.06 Policy to Assure Confidentiality, Integrity and Availability of DHMH Information (IAP).

**B) LA Information Technology (IT) Infrastructure and Security**

MDH Office of Information Technology (OIT) and LA Office of Information Management System (OIMS) are responsible for maintaining and supporting IT infrastructure and cybersecurity, including but not limited the following:

- a) Computer and system safety and security management
  - (1) Security firewall protection,

- (2) Computer Virus/Malware protection,
  - (3) Security patch management, and
  - (4) Disaster Recovery management.
- b) Computer and Network Access management
- (1) Computer and Network access authentication and authorization
    - i. Account management,
    - ii. Password Policy, and
    - iii. Access denial policy,
  - (2) Remote access protection, and
  - (3) Access denial procedures.
- c) Data safety and security management
- (1) Data classification hierarchy,
  - (2) Data encryption policy,
  - (3) Web data sanitization, and
  - (4) Data backup and recovery policy.
- d) Device safety, accountability and security management
- (1) In facility safety and security management,
    - i. Hardware assets management,
    - ii. Hardware inventory management.
  - (2) Mobile device and data safety and security management,
    - i. Check-out / Check-in policy,
    - ii. Password protection and Data encryption policy,

iii. System update policy, and

iv. Lost and Report policy.

e) **Safety and Security Auditing management**

(1) Security Board,

(2) Self-auditing Procedure and Plan, and

(3) Collaboration with MDH OIT Auditing

## II. Physical Security

### A) Access to Maryland Department of Health, J. Mehsen Joseph Public Health Laboratories Administration, Central Lab, 1770 Ashland Ave., Baltimore, MD 21205

- a) 1770 LA is a restricted building under 24/7/365 video surveillance.
- b) 1770 LA is operated as State Property and managed by Brookfield Properties. State Law, Code of Maryland Regulations, COMAR 04.05.01.03B specifies “Except for official purposes and by authorized personnel, an individual on the property may not carry open or concealed firearms, explosives, incendiary devices or dangerous or deadly weapons.”
- c) LA employees, authorized Brookfield Properties employees and A-tek and LA couriers’ may gain access by presenting an authorized Central Lab Photo ID Keycard at the time of entry.
- d) All visitors (e.g. other state, federal and county employees, contractors, non-routine couriers, employees’ relatives, vendors, service technicians, etc.) with legitimate business to conduct with the Laboratories Administration may gain access by:
  - (1) Presenting and turning over their current government-issued photo ID (i.e., driver’s license) to Brookfield Properties Security Officer posted at the Lobby;
  - (2) Verifying visitor has a “Visitor Clearance Sheet,” Appendix A.
  - (3) Signing-in at Lobby Security Desk on arrival;
  - (4) Obtaining and visibly wearing a dated “visitor’s” badge;
  - (5) Waiting for an escort from the lab or office to be visited; and
  - (6) Signing out at Lobby Security Desk and retrieving their government-issued photo ID on departure.

## **B) When Building Access May be Obtained**

- a) Twenty-four (24) hours, seven (7) days a week access is granted to select emergency essential LA employees and Brookfield Properties facility and engineering staff.
- a) Between 8:00 a.m. – 4:30 p.m. Monday through Friday, except State Holidays and State Service Reduction Days, are normal operational hours. (Director approved selected lab units with hour-after schedules are exempt.)
  - (1) Visitors – must first report to Lobby Security Desk [Following procedure in Section (A); Access to Central Lab 1770, subsection (d), parts 1-5.]
- b) Loading Dock and Alley Gate standard hours are 8:00 a.m. — 6:30 p.m. Monday through Friday, except State Holidays and State Service Reduction Days.
  - (1) Routine laboratory couriers who pick up reports, supplies and deliver laboratory specimens and samples, etc. shall be cleared for dock entry by the Loading Dock Monitor, at 443-681-3807. Once cleared, couriers will report to the Laboratory Receiving Office (Room 141) on the Lower level, adjacent to the Loading Dock.
  - (2) Routine delivery of purchases shall be made to the Warehouse 8:00 a.m. –4:30 p.m. Monday through Fridays, except State Holidays and State Service Reduction Days.
- c) Loading Dock and Alley Gate standard hours on Saturdays, State Holidays and State Service Reduction Days are 7:30 a.m.—10:30 a.m.
- d) Loading Dock and Alley Gate after-hours and emergency access
  - (1) Pre-approved LA couriers will use their Courier Photo ID Keycard to gain access to gate and specimen/sample drop-off locations.
  - (2) Pre-approved A-tek couriers will use the gate intercom to gain access to the locking dock, and their A-tek Courier Photo ID Keycard to gain access to the “All hazard Receiving and Chain of Custody Room.”
  - (3) Emergency receipt of specimens/samples for selected lab units, i.e., Select Agent Program (SAP) or Ebola testing, LA staff members must notify security of pending delivery to facility gate access. Pre-determine specimens/sample must be received at the “All Hazard Receiving” locking dock door.

## **C) Emergency Evacuation**

- a) All employees are to follow the Brookfield Properties Tenant Handbook (Appendix K, section 3 “Emergency Procedures,” Appendix B-Emergency Evacuation Procedure and Map, and Appendix D-Bomb Threat Report Form.)

b) Following a fire emergency, fire drill, bomb scare, explosion, or other emergency evacuation, all returning employees and visitors must re-enter the 1770 building only at the employee entrance Lobby on Rutland Ave. and follow procedures stated in Section (A) above: Access to Central Lab 1770. All persons re-entering the building must show a proper form of ID (employee's Photo ID Keycard; visitor badge). Persons failing to display a valid form of identification will not be re-admitted to the building.

c) Shelter-In-Place Procedure

Announcement will be made over the building's intercom system by SSO, Property Manager, LA Director, or designee with instructions for proper response. Employees should seek shelter in a room where the windows are not exposed to the exterior and close doors. Windowless corridors, conference rooms, and storage closets could be used as a room to "Shelter-In-Place". All LA employees are to follow Brookfield Properties Tenant Handbook for Shelter-In-Place Procedures.

#### **D) Suspicious Package**

a) All LA employees should inspect all packages and items before they are brought into or removed from LA.

b) All package should be inspected visually or by non-invasive techniques. Consider the following indicators of a potential suspicious package:

- (1) Misspelled words;
- (2) Addressed to a title only or an incorrect title;
- (3) Badly taped or sealed;
- (4) Lopsided or uneven;
- (5) Oily stains, discoloration, or crystallization on the wrapper;
- (6) Excessive tape or string;
- (7) Protruding wires;
- (8) Return address does not exist or does not make sense.

c) Follow the following produce for handling a potential suspicious package:

- (1) Once a package has been identified an suspicious – **DO NOT MOVE IT.**

- (2) Call 3911 notify security officer on duty there is a suspicious package AND clear the area.
  - (3) Wait for further instructions from the security officer, or designee, in an alternate safety and secure area away from the suspicious package.
- d) Suspicious package found left in or around the building will be referred to SSO, Brookfield Properties Security, and other appropriate law enforcement.

## **E) Active Shooter/Assailant Awareness**

- a) Due recent Active Shooter/Assailant events nationally and internationally, Laboratories Administration is providing with following advisory guidelines from United States Department of Homeland Security.
- b) Disclaimer: This information is advisory in nature and is NOT intended to identify all scenarios or situations when, where, and how an Active Shooter/Assailant or another emergency event is to take place. It is suggested that individuals follow his/her instincts. These guidelines will not guarantee your safety.
- c) An “active shooter” is an individual who is engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearm(s) and there is no pattern or method to their selections of victims.
  - (1) Victims are selected at random.
  - (2) Event is unpredictable and evolves quickly.
- d) United States Department of Homeland Security, “Active Shooter Event – Reference Guide,” recommends three (3) steps approach for what individuals, employees, can do:
  - (1) Run
    - i. Have an escape route and plan in mind;
    - ii. Leave your belongs behind;
    - iii. Evacuate regardless of whether others agree to follow;
    - iv. Help others escape, if possible;
    - v. Do not attempt to move the wounded;
    - vi. Prevent others from entering an area where the active shooter may be;

- vii. Keep hands visible; and
- viii. Call 911 when you are safe.

(2) Hide

- i. Hide in an area out of the shooter's view;
- ii. Lock door or block entry to your hiding place;
- iii. Silence your cell phone (including vibrate mode) and remain quiet;

(3) Fight

- i. Fight as a last resort and only when your life is in imminent danger;
- ii. Attempt to incapacitate the shooter;
- iii. Act with as much physical aggression as possible;
- iv. Improvise weapons or throw items at the active shooter; and
- v. Commit to your actions, your life may depend on it.

## **F) Security Barriers, Video Surveillance System, and Access Control Database**

### a) Security Barriers

- (1) Public access to 1770 is restricted to current employees, and approved contractors/visitors badges, with a photo ID keycard, electronic proximity (prox) card.
- (2) LA main entrance is manned by a Brookfield Properties security officer 24/7/365. In addition, there will be routine patrols of the building and grounds by security officers.
- (3) All perimeter doors, stairwells, open and closed lab work areas, and corridors require electronic prox card to enter. In addition, Biological Select Agent and Toxin (BSAT) areas require a prox card and PIN access.
- (4) In the event of emergency evacuation, power failure, or emergency, all doors will operate as "fail secure" allowing for LA Staff and/or visitors to exit the area, but prevents re-entry until the "all clear" has been issued.

### b) Video Surveillance and Access Control

- (1) The video surveillance system monitors MDH LA 24/7/365 with overt and covert cameras positioned internally and externally around the facility.
  - i. LA system video surveillance system is maintained and controlled by the SSO and BP Security Supervisor.
  - ii. Routine video footage is saved and stored on the security system servers and DVR.
  - iii. Video footage may be pulled to aid security investigations with written authorization from Brookfield Properties Security Director, Baltimore Police Department, Responsible Official and LA Director.
- (2) LA Access control system runs on a stand-alone network maintained by LA OIMS staff and SSO.
- (3) Access Control System Data Back-up – The security computers automatically perform cardholder database back-up twice a week and overwrite previous back-up data. The security system will continue to function if either workstation (redundant systems located at the Lobby Security Desk, Security Supervisors Office, and SSO Office) is out of service.
- (4) Access control system (C-Cure), Intercom system (Commend), video surveillance (Genetec System) provide progressive alarm integration coupled with 24/7/365 Brookfield Properties security officer presence constitute MDH LA's intrusion detection system.

## **G) Access to Biological Select Agent and Toxin (BSAT) Work and Storage Areas**

### **a) Roles of Responsible Official (RO).**

- (1) The Responsible Official (RO) is the individual designated by the registered entity with the authority and responsibility to act on behalf of the entity to ensure compliance with the select agent regulations. There can be only one RO at a registered entity at any given time. In the absence of the RO, a previously appointed and approved Alternate Responsible Official (ARO) may assume the RO's responsibility and has the authority to act on behalf of the registered entity. The core responsibilities of and criteria to be the RO are listed below:
  - i. The RO must have passed a security risk assessment (SRA) conducted by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) and be approved by the Federal Select Agent Program.



- ii. The RO must be familiar with the select agent regulations to the extent that the RO can ensure that his or her entity is compliant with all of the requirements of the select agent regulations.
- iii. The registered entity must not only assign the RO the responsibility to ensure compliance with the select agent regulations, the entity must also ensure that it delegates to the RO sufficient authority to speak and act on behalf of the entity. A registered entity which fails to vest in its RO sufficient authority to ensure compliance with all of the requirements of the select agent regulations has failed in one of its primary responsibilities.
- iv. The RO is responsible for ensuring compliance with Animal and Plant Health Inspection Service/Centers for Disease Control and Prevention (APHIS/CDC) Select Agent Program regulations, including:
  - 1. Developing and implementing safety, security and emergency response plans;
  - 2. Allowing only approved individuals to have access to select agents or toxins;
  - 3. Providing or ensuring appropriate training for safety, security and emergency response is provided;
  - 4. Transferring select agents or toxins;
  - 5. Providing timely notice of any theft, loss, or release of a select agent or toxin; and
  - 6. Maintaining detailed records of information necessary to give a complete accounting of all activities related to select agents or toxins.
- v. The RO must ensure that annual inspections are conducted for each laboratory and all other registered areas where select agents or toxins are stored or used in order to determine compliance with the requirements of the select agent regulations. The results of each inspection must be documented, and any deficiencies identified during an inspection must be corrected.
- vi. The RO must have a physical (and not merely a telephonic or audio/visual) presence at the registered entity to ensure that the entity is in compliance with the select agent regulations and be able to respond in a timely manner to onsite incidents involving select agents and toxins in accordance with the entity's incident response plan.

b) Policies Covering Employees in the BSAT Program

(1) Security Risk Assessment (SRA) - Prior to being granted access to select agents or toxins, an employee must first undergo a Security Risk Assessment (SRA) as defined in 42 CFR 73.8. The SRA is comprised of completing and submitting the Federal Bureau of Investigation (FBI), Bioterrorism Preparedness Act: Entity/Individual Information (FD-961) form and two sets of fingerprints on FBI fingerprint cards (FD-258) to the FBI Criminal Justice Information Services division (CJIS) through the Responsible Official (RO) or Alternate Responsible Official (ARO). Employee may be denied access to select agents or toxins if they:

- i. Are a restricted person under United States Code (U.S.C.), Title 18, Part 1, Chapter 10, §175b,
- ii. Committed a crime specified in 18 U.S.C. 2332b(g)(5),
- iii. Have knowing involvement with an organization that engages in domestic or international terrorism (as defined by 18 U.S.C. 2331) or with any other organization that engages in international crimes of violence, or
- iv. Are an agent of a foreign power (as defined in 50 U.S.C. 1801).

(2) Minimum education experience, and training: To be granted BSAT access an employee will:

- i. Meet State's Personnel minimum qualifications for a Public Health Laboratory Scientist or a Public Health Laboratory Technician functioning in high containment labs; and
- ii. Have effectively completed and documented on-the-job training in the safe and proper handling of BSAT, as needed.

c) Policies Covering Non-BSAT Employees

(1) Escort Requirements:

- i. An approved BSAT employee shall accompany, at all times in an area containing a select agent or toxin, an individual not approved to work with or have access to select agents or toxins.
- ii. BSAT employee must escort all cleaning and preventive maintenance staff, instrument repair workers and contractors.
- iii. Escort may do no other work other than escort the non-SRA approved employee.

(2) Removal of unauthorized personnel:

- i. No unapproved individual may visit an area containing a BSAT without the prior approval of the Principal Investigator (PI) and without being escorted by an SRA-approved individual at all times while in the area.
- ii. An employee who observes the presence of an individual not authorized to be in an SAP-registered area will treat the individual's presence as a breach in security. The employee will immediately notify the Lobby Security Guard at 443-681-3795, the Safety and Security Officer, the RO and/or ARO.

d) BSAT Inventory Controls

- (1) Each BSAT-registered laboratory will require that freezers, refrigerators, cabinets, and other containers where stocks of select agents, toxins, or both are stored be kept locked when not in direct view of SRA-approved staff, and will be subject to other monitoring measures such as video surveillance when needed.
- (2) Access Controls for Containers Storing BSAT: An employee with access to BSAT will comply with the access controls set forth in the SOPM covering each laboratory and storage area where a BSAT is stored.
- (3) Inventory Documentation and Records Policy: An employee with access to BSAT will comply with inventory policy and procedures set forth in the SOPM covering each laboratory where a BSAT is stored.
- (4) Intra-Entity Transfer of Select Agents and Toxins: An employee with access to BSAT will comply with the Laboratories Administration's policy covering the intra-entity transfer of a BSAT by:
  - i. Carrying out such a transfer only with the knowledge and approval of the PI, RO, immediate supervisor; and
  - ii. Completing appropriate transfer log and inventory records associated with the BSAT at the time of transfer.
- (5) Examination of Packages Entering and Exiting BSAT Containing Areas:
  - i. A suspicious package (as defined in the *Security Guidance for Select Agent or Toxin Facilities*, page 24.) being brought into an SAP-registered storage or work area will be examined by an SAP-approved Laboratories Administration scientist at the time of entry for the presence (transfer) of select agents and, if present, immediately will be properly inventoried and stored. Also, refer to section **XIII. Inspection of Packages**

- ii. Prior to preparing (wrapping) a package for removal from the area (other than what is generated during normal daily operations, i.e., supplies, autoclaved waste) an SAP-approved Laboratories Administration scientist will document that they:
  1. Examined the contents of the package for the presence of a BSAT;
  2. That, on finding an agent for transfer, proper approvals were obtained, proper transfer forms were completed, and inventory records updated; and
  3. Decontaminated the package according to the procedures in the BioSafety Level-3 (BSL-3) SOP.

e) BSAT Physical Security—Access Control

(1) Intrusion Detection and Alarms-- In the event of a physical breach or closure failure of a door to a BSAT registered room, the security system will sound a priority-one alarm at the guard's monitoring station at the Lobby Security Desk (24/7/365). The guard will notify Brookfield Properties Security for immediate response. The response time for security forces or Brookfield Properties Security will not exceed 15 minutes (The response time is measured from the time of an intrusion alarm, or report of a security incident, to the arrival of the responders at the first security barrier.) The security officer will call SSO and OLEPR emergency phone.

- i. All Priority 1 Alarm events will be fully investigated and documented (including the use of door records and video to determine the cause of the alarm).

(2) Power Failure— In the event of a power failure, the security doors and security computers have a battery back-up to bridge the outage until the back-up generators re-energize the 1770 building. If the power fails, the doors to the BSAT-registered rooms will operate as "fail-secure." This allows employees inside the BSAT registered area to exit the room during/after a power outage but prevents access (entrance) to the room.

## H) Waste Storage and Removal

- a) Lab generated hazardous waste, special medical waste/biohazard waste, and radiation waste materials are stored in segregated secure storage rooms until the waste can be scheduled for removal and disposal.
- b) The LA must contract or hire a licensed and permit holding waste hauler that is in good standing with State and Federal regulators to package, ship, haul, and dispose of hazardous waste, special medical waste/biohazard waste, or radiation waste generated at their facility.

## **I) Packaging and Shipping Dangerous Goods**

- a) For guidance and regulations for shipping dangerous goods, Classification 6, Hazard Class 6: Toxic and Infectious Substances, Division 6.1 Poisonous Material and Division 6.2 Infectious Substances, consult current policies and procedures from Department of Transportation (DOT), International Air Transportation Association (IATA), and United States Postal Service (USPS).
- b) Only trained and certificated LA staff are authorized to package and ship samples or specimens, or any materials considered Classification 6, Hazard Class 6: Toxic and Infectious Substances, Division 6.1 Poisonous Material and Division 6.2 Infectious Substances either Category A or B.
- c) Staff should also refer to their divisional standard operating procedures for packaging and shipping.

## **J) Role of Safety and Security Officer**

- a) Security Training: The SSO, or designee, will provide security awareness training and orientation for new employees within the first month of employment. Ongoing security training will be provided at least annually to all employees and more often if needed.
- b) Access Control: The SSO will respond to written requests for additions, changes or deletions to the access control system database from LA Director or designee. All written requests must have the proper approval signatures. The SSO will maintain copies of all requests.
- c) Acts as the Laboratories Administration's liaison with Brookfield Properties Security.
- d) Responds to reports of security breaches.
- e) Acts as the biosafety and biosecurity officer for the BSAT Program, and provides support to the Laboratories Administration OLEPR.
- f) Annually, and following a reported security incident or breach, undertake a functional security review.
- g) Responsible for maintaining Laboratories Access Control System and Video Surveillance System.

## **K) Brookfield Properties Security Officers Posted at 1770**

- a) First Floor Lobby Security Desk

(1) Hours of Operation

- i. 24/7/365 is manned by at least one Security Guard, 443-681-3795.
- ii. During the Dayshift 7:00 AM to 4:30 PM, the Lobby Security Desk is manned by two (2) security guards.

b) Loading Dock Security Desk and Loading Operations

(1) Security Desk Hours of Operation

- i. Monday through Friday, 7:00 AM to 6:30 PM, the Loading Dock Security Desk is manned by one guard, 410-350-6390.

(2) Loading Dock Security Officer Role

- i. The officer shall not sign or receiving any packages.
- ii. For visitors or couriers, Officer must contact a LA employee to be an escort.

(3) Loading Dock Operations

- i. Routine deliveries of purchases shall be made to the Laboratory Receiving Office, 8:00 AM to 4:30 PM, Monday through Friday, except for Service Reduction Days and State Holidays.
- ii. 7:30 AM to 10:30 AM, Saturdays, Service Reduction Days, and State Holidays- laboratory couriers will deliver laboratory specimens or samples to Room 141, Courier Drop Off. Couriers shall notify Data entry or Accessioning, or designee by phone of their arrival.

- c) Brookfield Properties Security is responsible for maintaining security staff at Lobby Security and Loading Dock Security Desk.
- d) All Brookfield Properties Security staff must adhere to all Brookfield Properties Security management policies and procedures.
- e) All security staff problems or concerns must be brought to the attention of the SSO and Brookfield Properties Security Management, 410-900-1040.

**L) Brookfield Properties Security Enforcement of Security Plan**

- a) Enforcement of 1770 Access and Visitor Policies:

- (1) Security Officer shall verify visitor has completed Visitor Clearance Sheet, Appendix A. and contact the escorting staff member;
  - (2) Collect visitor current government-issued photo ID (i.e., driver's license);
  - (3) Sign visitor in and out;
  - (4) Assign Visitor badge with lanyard: Officer will ensure all visitors properly obtain, wear, and return visitor's badge.
  - (5) Employee Escorts: Officers will prohibit visitors from traveling beyond the Officer's post unless escorted by a LA employee.
  - (6) Removal of State Property: Officer shall question, ask for State Property Pass, from any LA employee. Officer shall contact SSO or Inventory Control Officer, 443-681-3820.
- b) Provide security input to LA Safety and Security Committee. Brookfield Properties Security Officers shall report any safety and security concerns to SSO and Brookfield Properties Security Manager.

#### **M) Brookfield Properties Security Officer- LA Employee Interactions**

##### a) Incident Reporting

- (1) 1770 Security Staff shall immediately report any security incident, breach, or suspicious activity to SSO and Brookfield Properties Security.
- (2) 1770 Security Staff shall immediately report any security incident, breach, or suspicious activity that may be criminal in nature involving BSAT areas to SSO (443-681-3792), RO/ARO (cell: 410-925-3121; office: 443-681-3789), and Brookfield Properties Security Office.
  - i. 1770 Security Staff will complete Security Incident/Breach Reporting Form, Appendix C.

##### b) Alarm Notification

###### (1) BSAT Priority 1 Alarms

- i. Priority 1 Alarms, include but are not limited to BSAT registered areas; perimeter areas entry and egress—elevators, doors, and stairwells; data closets, and other area high-security areas.
- ii. Require immediate notification and investigation within 15 minutes of the alarm event by Brookfield Properties Security staff 365/24/7.

- iii. Lobby Security Office must contact SSO (443-681-3792), RO/ARO (cell: 410-925-3121; office: 443-681-3789), and Brookfield Properties Security Office.

(2) Secondary Alarms must be acknowledged and recorded into the access control system.

c) LA Resource and Reference Materials for Lobby and Loading Dock Security Desk

(1) SSO or designee will provide the current copies of following materials:

- i. LA telephone directory,
- ii. LA organization chart,
- iii. LA floor plans and lab locations, and
- iv. LA’s “Guide to Public Health Laboratory Services.”

d) Equal Treatment and Enforcement of Administration's Security Policies:

- (1) All employees and visitors are subject to the LA's security policies;
- (2) Brookfield Properties Officers posted at 1770 will challenge any employee disregarding established security protocols. An incident report will be completed documenting breach in security.
- (3) Any on-going breach of security issues involving an individual or individuals, will be communicated to the SSO and LA Director by the Brookfield Properties Security Management.

**N) LA Key Contacts**

<b>Title</b>	<b>Name</b>	<b>Location</b>	<b>Phone Number</b>
Director	Robert Myers, Ph.D.	128A	443-681-3801
Deputy Director, Scientific Programs	Vacant	238	443-681-3851
Deputy Director, Administrative, and Support Operations	Rodney Hargraves	128D	443-681-3802
Special Assistant	Donyet Barnes	128H	443-681-3939
Safety and Security Officer	Rachel Michael	132C	443-681-3792
Quality Assurance Officer	Heather Peters	132A	443-681-3791



Inventory Control Officer, Registration Supervisor	Denise Shackelford	132D	443-681-3820
Radiation Safety Officer	Wuernisha Tuerxun, Ph.D.	232	443-681-4696
Office of Information Management Services	Ruiwu Toa	132B	443-681-3780
Office of Laboratory Emergency Preparedness and Response (OLEPR) (Responsible Official)	Jim Svrjcek OLEPR call down list.....cell phone pager	134	443-681-3787
			410-925-3121 410-408-7521
Newborn and Childhood Screening Division	Fizza Gulamali-Majid, Ph.D.	324	443-681-3901 443-681-3900
Molecular Biology Division	Robert Myers, Ph.D.	128A	443-681-3801
Environmental Sciences Division	Vacant	238	443-681-3851
Microbiology Division	David Torpey, Ph.D.	536	443-681-3951
Virology and Immunology Division	Venkata R. Vepachedu, Ph.D.	424	443-681-3930

**O) Brookfield Properties Building and Security Key Contacts**

a) Brookfield Properties Security Key Contacts

- (1) 1770 Security/Emergency: 443-681-3911
- (2) Lobby Security Desk: 443-681-3795
- (3) Loading Security Desk: 410-681-3808
- (4) 855 Campus Security Office: 410-900-1002
- (5) Brookfield Properties Security Supervisor: 410-900-1002
- (6) Brookfield Properties Security Director: 410-900-1017

**P) Brookfield Properties Security Roles and Responsibilities**

a) Brookfield Properties Security Management is responsible for posting, training, and maintaining security guard staff at the Lobby Security Desk and Loading Dock Security Desk. Lobby Security Desk will be manned 24/7/365. Loading Dock Security Desk will be manned during operational hours. Additionally, a security officer will conduct routine interior and exterior patrols of the building and surrounding grounds.

- (1) Lobby Security Officers are responsible for:
  - i. Monitoring the access control systems, Ccure9000 and Intercom, and video surveillance system, Genetec, for alarms and daily transaction.

- ii. Enforcing of all LA and Brookfield Properties security policies.
- iii. Conducting after-hours perimeter and interior walkthrough, refer Brookfield Properties Security SOP.
- iv. Adhering to all Brookfield Properties Security memos, policies, and SOPs.

(2) Loading Security Officer is responsible for:

- i. Monitoring alley driveway and gate, loading bays, and loading area.
  - ii. Enforcing of all LA and Brookfield Properties security policies.
  - iii. Adhering to all Brookfield Properties Security memos, policies, and SOPs.
- b) Brookfield Properties Management will provide LA with any access control, service, maintenance, and operating reports upon request.
- c) Brookfield Properties Security Director is a member of the BSAT Program and subject to BSAT Program requirements.

## **Q) Metal Keys and Locks**

a) Locker Keys and Combination Locks

- (1) Upon employment, any LA employee who does not have an office will be assigned a locker and locker key or combination lock .
- (2) The employee will sign that he/she received the locker and locker key, see Appendix D "Locker Request Form."
- (3) LA Personnel Liaison, or designee, is responsible for maintaining locker assignments and locker keys.
  - i. LA Personnel Liaison, or designee, will maintain a confidential list of locker and locker key assignments. The list will contain employee's name, floor, unit, locker number, date of locker assignment, and date key was returned or reported lost or stolen.
- (4) Loss and Replacement Locker Keys
  - i. Loss of a locker key must be reported to the issuing party. Only the employee who was in legitimate possession of the key may request a replacement.

b) Room Keys and Other Keys

- (1) Requests for employees to receive metal door keys to individual offices must be in writing by employee's Division Chief and approved by the Director. See Appendix E "Key Request/Receipt Form." Approved and signed forms are submitted to and maintained by SSO.
- (2) Fleet Manager maintains key(s) to LA State Car.
- (3) File cabinet keys or lock-box keys, are maintained by the Division Chief or his/her designee.

c) Combinations and Locks

- (1) Authorization: Requests for changes to combinations or locks must be made in writing to, or through, a Division Chief, or designee, to SSO.
- (2) Announcement: Before a new combination or lock change is implemented, the Division Chief will inform employees with a need to know of the change and will support the change by working with the SSO.

**R) 1770 Photo ID Keycard**

a) New LA Employees

- (1) New employee's supervisor must submit a "MDH 1770 Building Keycard Request and Access Form" to SSO to have the employee added to the access control system, see Appendix B.
- (2) Upon approval, the new employee will then be issued a photo ID keycard that will provide entry to 1770 and, if appropriate for employee's duties, will also allow access to one or more sensitive laboratories or offices.
- (3) Access Level Change: The procedure outlined above should also be used anytime there is a change in an employee's access level for sensitive areas or offices.

b) 1770 Photo ID Keycard Holder Responsibilities

- (1) Wear their Photo ID Keycard: The building security requires all LA employees to wear their 1700 Photo ID Keycard to move throughout the building, and to enter or exit the building.
- (2) Use of Card Readers and Pin Code Card Readers: Employee must present their 1770 Photo ID Keycard at the proximity (prox) card reader or prox pin code card reader to "Badge in" for that door each and every time he/she enters, or exits, the door.

- (3) Deactivated Lock: If an employee has already deactivated the lock by presenting their Photo ID Keycard at the reader and has opened the door, each subsequent employee must also present their own card to the card reader before entering the door, even if the door is open.
- (4) Lock deactivated by motion detector: An employee entering a door, which has had the lock deactivated by motion on the opposite side of the door, must present their Photo ID Keycard at the prox reader before entering.
- (5) Ensuring that others Present Photo ID Keycard: An employee, who has badged in to enter a door and, to be courteous, is holding the door open for a fellow employee, must ensure that the fellow employee also presents their badge to the reader before entering. If the fellow employee refuses to badge in, he/she must be reported to the SSO or Security Officer.
- (6) Piggybacking: Entering a door, without badging in, that is being held open by another employee [who has badged in], is called piggybacking. This is a violation of the LA's security policy.
- (7) Employees Without Their Photo ID Keycard: Employees, who do not have their Photo ID Keycard must use the intercom for access and report to the Lobby Security Desk, sign in and receive a Visitor's Badge. They must not enter on another employee's badge. If their Photo ID Keycard has been lost or stolen they must notify the SSO immediately.
- (8) Refusing Access to Unauthorized Persons: An employee with 1770 Photo ID Keycard access should not allow a State Employee outside the Administration or a visitor without card access to piggyback on their badge. LA employee must escort the perspective visitor to the Security Desk.
  - i. An employee who is apprehensive about confronting a visitor or fellow employee who insists on piggybacking must report the violator to the Security Desk Officer or contact the SSO.
- (9) Access Limitation: 1770 Photo ID Keycard may not be loaned by one employee to another or to a non-Administration employee
- (10) Reporting Improper Use: An employee noticing improper use of any Photo ID Keycard by an unauthorized person must immediately notify their immediate supervisor and SSO.

c) Stolen, Lost, Damaged or Forgotten employee 1770 Photo ID Keycard

- (1) Stolen or Lost 1770 Photo ID Keycard: An employee must report lost and stolen 1770 Photo ID Keycard immediately to the Brookfield Properties Security Guard and SSO. In addition, if the employee is part of BSAT program, the RO and Lab Director must be notified.
  - i. Stolen Photo ID Keycard: An employee must provide the SSO with a copy of police report, or other police official documentation, as a record of the theft.
  - ii. 3-Strikes Lost Photo ID Keycard Policy  
Once an employee has lost their Photo ID keycard three (3) times he/she will be charged \$50.00 to replace the third ID.
- (2) Damaged 1770 Photo ID Keycard: An employee must report the damaged ID to their supervisor and SSO immediately. Employees are not responsible for the cost of replacing damaged ID.
- (3) If an employee forgets their Photo ID keycard the employee must turn over their government-issued photo ID, i.e., driver license, to the Lobby Security Officer at the start of their work day in order a temporary keycard. The employee will sign-out for their temporary keycard. At the conclusion of the employee's work day, he/she will turn-in temporary keycard to Lobby Security Officer and retrieve their government-issue photo ID. Failure to return the temporary keycard will result in documented progressive discipline. (Temporary keycard will not be issued to BSAT areas.)

d) Employee Separation:

- (1) An employee terminating employment from the LA must turn in all keys and IDs (including their 1770 Photo ID Keycard and Maryland State Employment ID) to the LA Personal Liaison or SSO prior to separation.
  - i. The following items must also be turned into the SSO, LA Personal Liaison, or designee:
    1. Employee Binder,
    2. All three (3) assigned lab coats,
    3. Locker key, and/or
    4. Office key.
- (2) Prior to the employee's last day of work, the LA Personnel Liaison will provide his/her supervisor with the "MDH Employee Offboarding Supervisor's Checklist" see Appendix F. Once the supervisor receives the "MDH Employee Offboarding Supervisor's Checklist" he/she must provide the form to their employee within 24 hours. All

separating LA employees are required to complete the “MDH Employee Offboarding Supervisor’s Checklist.” The completed form is returned to the LA Personnel Liaison.

(3) SSO will disable the employee badge in the access control system.

(4) OIMS Chief, or designee, will remove the employee from network access, and archive the employee’s email address.

**S) Policy and Procedure for LA Employee without a government issued photo identification needing a TEMP keycard.**

- a) If a LA employee arrives at the 1770 Ashland Avenue facility during normal business hours, M-F 7:00 a.m. – 4:30 p.m. without a government issued photo identification BP Security must complete Appendix L “Laboratories Administration Employee Temporary Keycard Authorization Form.”
- b) The “Laboratories Administration Employee Temporary Keycard Authorization Form” must be completed and signed by the employee’s divisional supervisor/manager/division chief, LA Personnel Officer, SSO, or QAO and the LA employee for BP Security to issue a TEMP keycard. The purpose of this form is to ensure the individual requesting a TEMP keycard is a current LA employee in good standing.
- c) BP Security shall not be permitted to issue TEMP keycard to LA employees after-hours, weekends, or holidays without a government- issued photo identification. LA employees must contact their supervisor and return to work with proper government- issued photo identification.

**T) Maryland State ID**

a) Department of General Services (DGS), Maryland Capitol Police Badge Office

(1) DGS, MD Capitol Police Badge Office is responsible for distributing all Maryland State Employee ID.

i. Location: State Center, 201 Building, 201 W. Preston Street, Baltimore, MD 21201.

ii. Hours: Monday through Friday, 8:00 a.m. to 3:00 p.m., closed between 12:00 and 1:00 p.m.

b) Maryland State Employee ID and Employee Responsibilities

(1) State Employee ID is considered State property.

- i. Employees separating from State service (i.e., retiring, resigning, or terminated) must turn in their Maryland State Employee ID on their last day of employment to their supervisor or the SSO.

(2) Full-time and permanent MD State Employees may use their State Employee ID to ride Maryland Transit Administration (MTA) public transportation (i.e., Light Rail, Metro Subway, and MTA Buses) for free.

(3) SSO is the LA Maryland State Employee ID Badge Coordinator at 1770.

c) New Employees

(1) New employees will receive their Maryland State Employee ID at New Employee State Orientation. LA Personnel Liaison will contact employee's supervisor to schedule New Employee State Orientation.

d) Stolen, Lost, or Damaged Maryland State Employee ID

(1) Stolen or Lost Maryland State Employee ID: An employee must report lost and stolen Maryland State Employee ID immediately to Brookfield Properties Security Guard and SSO.

- i. Stolen Maryland State Employee ID: An employee must provide the SSO with a copy of police report, or other police official documentation, as a record of the theft.

- ii. Lost Maryland State Employee ID

1. DGS, MD Capitol Police charges for replacement ID: First-time replacement cost for lost ID is \$50.00, the replacement cost of the 2<sup>nd</sup> ID is \$100.00, and 3<sup>rd</sup> replacement ID cost \$250.00.
2. DGS, MD Capitol Police will accept only checks or money orders payable to Dept. of General Services. Cash will not be accepted.
3. A photo ID, such as a Maryland Driver's License, Maryland MVA Identification Card, Passport, or Current Military ID card must be shown to process the new request.

(2) Damaged and Loaning Maryland State Employee ID: An employee must report the damaged ID to their supervisor and SSO immediately. Employees are not responsible for the cost of replacing damage ID. Maryland State Employee ID may not be loaned by one to another or to a non-State Employee. Employees found to have loaned a Maryland State ID are subject to arrest and termination of State employment.

## U) State Property Passes

- a) State Property Passes: Loading Dock Monitor will enforce the use of property passes for any State owned equipment temporarily being taken out of 1770 by employees and visitors.
- (1) Two (2) original passes authorized by Lab employee’s supervisor must be obtained. One original signed pass is to be given to the Loading Dock Monitor. The second pass with original signatures is to remain with the equipment. (Passes may be downloaded: [www.dgs.state.md.us/property pass](http://www.dgs.state.md.us/property_pass)).
  - (2) Collected property passes shall be reviewed and maintained at the Loading Dock Monitor’s Desk. The LA’s Inventory Control Officer will obtain a copy of passes at the end of each month.
  - (3) LA Inventory Control Officer shall maintain inventory records and State Property passes, in adherence to MDH Laboratories Administration’s *Records and Disposal Schedule*. (Department of General Services –State Records Center Schedule Number 2582, pg. 1-20, “DHMH Laboratories Administration This Schedule Supersedes Schedule 220.”)
  - (4) Each LA Division has a Property Accountable Officer:

Divisional Property Accountable Officers			
Division	Accountable Officer	Location	Ext.
Administrative Services & OIMS	Carlton Jennings	OIMS Workstation	443-681-3783
Billing, Lobby Offices, Registration, Outfits Prep, Maintenance, OLEPR, QA, Safety, & Prep Lab	Cynthia Queensbury	133A	443-681-3819
Newborn Screening/NBS Follow Up	Mark Taylor	325	443-681-3912
Division of Environmental Sciences	Yolanda Simms	LL11/237	443-681-3763
Division of Microbiology	Valarie Johnson	548	443-681-3942
Division of Molecular Biology	Veronica Adams-Landon	333	443-681-3924
Division of Virology/Immunology	Kenneth Okogi	420 B53A	443-681-3932 443-681-3770
Labs Administration Property Officer	Denise Shackelford	132D	443-681-3820

## III. Security Policies



## A) Visitors in the Workplace Policy

### a) Purpose

To improve security and safety for employees, laboratories, and offices in the MDH, J. Mehsen Joseph Public Health Laboratories Administration, Central Lab, located at 1770 Ashland Ave. Baltimore, Maryland.

### b) Background

Due to the nature of work performed in the LA 1770 facility and the number of visitors accessing the complex in an unofficial capacity, a visitors' policy is necessary due to concerns relating to work disruption, health, safety, and liability. This policy seeks to be mindful of employees' interests, other employees who may be adversely impacted, and the State's liability in the event of injury to the visitor or damage caused by a visitor.

### c) Policy

The basic principle of security is to limit access to assets based upon need. When protecting information, for example, access to documents should be limited to those persons with a need to know the information. When the asset to be protected is a room, an area, a building, a computer, or other such property, access to that property should be restricted to those persons who, due to their official duties and/or responsibilities, have a need for such access. Therefore, the following guidelines for visitors will be adhered to:

#### (1) Tours

LA tours are only permitted after the Director or designee, and the Training Coordinator, approve the request. A written tour request must be submitted to the Director, or designee, and the Training Coordinator for approval. Once approved, the Training Coordinator submits a Tour Sign-in Sheet to Lobby Security. Each tour member must present photo ID to gain entrance to the facility.

#### (2) Visitors

- i. All visitors to LA 1770 facility must be approved by a supervisor, or the designated appointed authority, to conduct legitimate State business. (Refer to the previously mentioned language in II) A) d) must be followed. Additionally, refer to section iv. Employee Family Members and Friends for personal visitors' procedures.)
- ii. "Visitor Clearance Sheet," Appendix A must be completed and given to the Lobby Security Officer. Procedures previously mentioned in II) A) d) must be followed.
- iii. Visitors with no advanced notice:  
In some cases, it is not possible to schedule visitors in advance. Although their names will not be on the Daily Visitor Log Book, clearance can be authorized through a contact employee. Visitors will be required to present a photo ID to gain access. Visitors will also be required to provide name and telephone

number of Lab employee for an employee escort. The LA employee escorting the visitor must obtain written authorization from their supervisor, or the designated appointed authority, for any unannounced visitor prior to his/her entry.

iv. Employee Family Members and Friends

Family members and friends should limit visits to the LA 1770 Facility and shall not be allowed in technical work areas. These visits shall not be for extended periods or be disruptive to other employees. Employees must get supervisor written approval for such visitor(s). **Children (under 18 years of age) are restricted to offices, visitor corridors, administrative areas, conference rooms, and restrooms. Children may not roam unattended through hallways. A responsible adult must attend them.**

1. Children are not permitted in technical or non-technical work areas for childcare reasons. Employees are responsible for arranging suitable outside childcare for their children during working hours.

v. Employees' Responsibility

Employees are responsible for ensuring all personnel adheres to all safety and security policies and procedures. Employees will be held accountable for all personal visitors' actions and property damage.

vi. Supervisors' Responsibility

Supervisors are responsible for ensuring employees comply with the LA visitor policy.

## B) Security Awareness

a) New Employee Orientation

Every new employee, as part of their LA orientation, shall complete a general security awareness orientation within the first week of employment, provided by the SSO that shall cover at least the following:

- (1) Distribution and review of LA Security Plan and Manual;
- (2) Review of emergency phones;
- (3) Review of security of confidential and sensitive records;
- (4) 1770 Photo ID Keycard Policy;
- (5) State ID Policy;

- (6) Visitor Policy;
- (7) Metal Keys or Locker Policy;
- (8) Perimeter security, limit access, and restricted access areas; and
- (9) Security incident reporting.

b) Security Orientation for Select Agents and Toxins

A new employee or transferring an employee who will be granted access to select agents or toxins also must complete a security orientation for select agents and toxins before being granted that access. BSAT Security orientation will be conducted by the RO/ARO and SSO.

IV. Appendix A Laserfiche Visitor Clearance Sheet

**Visitor Clearance Sheet  
Laboratories Administration**

**To:** Security Officer posted at the Lobby Security Desk, 443-681-3795

**From:** \_\_\_\_\_

**Unit:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Please add the following visitor to the 1770 Daily Visitors Log:**

\_\_\_\_\_  
**Date and time of arrival**

\_\_\_\_\_  
**Visitor's name**

\_\_\_\_\_  
**Company name**

\_\_\_\_\_  
**Destination within the facility**

\_\_\_\_\_  
**Purpose of visit (meeting, equipment repair, etc)**

\_\_\_\_\_  
**Employee escort and telephone number(s)**

**Please add visitor parking validation, see below signature approval:**

\_\_\_\_\_  
**Division Chief, Deputy Director, or Director**

\_\_\_\_\_  
**Signature**

Security Plan and Manual version 1.0 4/1/2015

# V. Appendix B 1770 ID Request, Separation, and Security Access Form

## Laboratories Administration ID REQUEST and SECURITY ACCESS FORM

Name ( Print ) Last : \_\_\_\_\_ First : \_\_\_\_\_ MI: \_\_\_\_\_

Date : \_\_\_\_\_

Unit /Division : \_\_\_\_\_ Lab/Office Phone #: \_\_\_\_\_

Supervisor (Print): \_\_\_\_\_ Supervisor(Signature) \_\_\_\_\_

Division Chief/  
Deputy Director  
(Print) \_\_\_\_\_ Division Chief/ Deputy  
Director (Signature) \_\_\_\_\_

Responsible  
Official/ Alternate  
Responsible Official  
(Print) \* \_\_\_\_\_ Responsible Official/  
Alternate Responsible  
Official (Signature) \* \_\_\_\_\_

Director (Print) Robert A. Myers, Ph.D. Director (Signature) \_\_\_\_\_

Justification: \_\_\_\_\_

**Contractor/MIPAR Employee:** Yes  No  Expiration Date: \_\_\_\_\_

**Parking:** Ashland Ave. Garage (Monthly Discount Rate) :  \_\_\_\_\_

**Required Access:**

Access Group/Lab:

General/Limited	IT Data Rooms	TB Lab BSL-3	A-Tek/Biowatch	Forest City Security
Bulk Storage	CT Lab	BSL-3 (1 <sup>st</sup> , 3 <sup>rd</sup> and 4 <sup>th</sup> Floors)	*Select Agent Program (SAP)	Forest City Engineering
Secure Record Storage	Radiation Lab	Rabies Lab (LL and 4 <sup>th</sup> Floor)	*Office of Laboratory Emergency Preparedness and Response	Forest City Cleaning

\*RO/ARO must sign off on all SAP access

-----  
**Employee PhotoID Keycard:**  New  Damaged  Lost  Access Update  Name Change  Renewal  Stolen

**Replacement cost for 3<sup>rd</sup> lost 1770 PhotoID Keycard is \$50.00. Checks or money orders will be accepted and should be payable to: DHMH Laboratories Administration. CASH WILL NOT BE ACCEPTED. A photo ID, such as a Maryland Driver's license, Maryland MVA identification card, Passport, or Current Military ID card must be shown to process this request.**

Applicant Signature: \_\_\_\_\_ Date: \_\_\_\_\_

-----  
 SSO or Designee  
 Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**For Official Use Only:**

Fiscal Supervisor Signature \_\_\_\_\_ Date: \_\_\_\_\_

SSO Signature \_\_\_\_\_ Date: \_\_\_\_\_

Date of Request: \_\_\_\_\_ Card #: \_\_\_\_\_ Inv. # \_\_\_\_\_

Agency Pay  Check  Money Order Amt: \_\_\_\_\_ Document #: \_\_\_\_\_

Version 2/26/2018

VI. Appendix C 1770 Security Incident/Breach Reporting Form

**Security Incident/Breach Reporting Form  
1770 Laboratories Administration**

Person filing report: \_\_\_\_\_ Date: \_\_\_\_\_ Time: \_\_\_\_\_

Person filing the report signature: \_\_\_\_\_

Supervisor who was informed: \_\_\_\_\_ Date Supervisor notified: \_\_\_\_\_

Location of incident: \_\_\_\_\_

Incident Summary: \_\_\_\_\_

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

Initial verbal report of incident given to: \_\_\_\_\_  
Forest Security Officer

Date: \_\_\_\_\_ Time: \_\_\_\_\_

A copy of this form was submitted to:

- Division Chief
- Director or Deputy Director
- Safety and Security Officer (SSO)
- Responsible Official/Alternate Responsible Official
- Office of Laboratory Emergency Preparedness and Response
- Forest City Security Supervisor

Incident reviewed by SSO: \_\_\_\_\_ Date: \_\_\_\_\_

Recommended follow-up: \_\_\_\_\_

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

**VII. Appendix D Locker Request Form**

**1770 MDH Laboratories Administration**

**LOCKER REQUEST FORM**

EMPLOYEE PRINTED NAME \_\_\_\_\_

PHONE # \_\_\_\_\_ DATE \_\_\_\_\_

FLOOR \_\_\_\_\_ LOCKER NUMBER \_\_\_\_\_

SUPERVISOR APPROVAL SIGNATURE \_\_\_\_\_

DIVISION CHIEF APPROVAL SIGNATURE \_\_\_\_\_

MUST BE SIGNED BY  
Laboratories Administration Personnel Liason  
(Or designee) \_\_\_\_\_

VIII. Appendix E MDH 1770 Building Key Request Metal Keys



**DHMH 1770  
Building Key Request  
Metal Keys**

<b>*Required field.</b>		
<b>*First</b>	<b>MI</b>	<b>*Last Name</b>
<b>*Primary Phone Number</b>	<b>Secondary Number</b>	
<b>Email Address (contractor only)</b>	<b>*Department/Company Name</b>	
<b>Driver License Number (contractors only)</b>	<b>Employee ID Number</b>	
<b>Key Distribution</b>		
<b>Qty</b>	<b>Key Description: (room number, door number, etc)</b>	<b>Key # if applicable</b>
<b>DHMH Division Chief Authorization (if applicable)</b>		
	<b>Signature</b>	<b>Date</b>
<b>DHMH Director or Deputy Director Authorization</b>		
	<b>Signature</b>	<b>Date</b>
<b>DHMH Safety/Security Officer Authorization</b>		
	<b>Signature</b>	<b>Date</b>
<b>Forest City Management Authorization</b>		
	<b>Signature</b>	<b>Date</b>
Mark McKinney		
<b><u>Terms and Conditions:</u></b>		
I understand that I have received the(se) key(s) on behalf of my company, which is named above. I understand that all keys must be surrendered to the DHMH Safety & Security Officer, and/or the Forest City Management, upon request or when my employment is terminated. Failure to return key will result in charges to replace the key and/or door locks that it operates.		
All keys are owned and controlled by DHMH and MEDCO (FCE, as agent), unauthorized key distribution or duplication is prohibited. All unreturned, lost or stolen keys must be reported <b>immediately</b> to DHMH Safety & Security Officer, and the FC Management.		
I, _____ hereby acknowledge receipt of key(s) for the above named company and have read and understand the terms and conditions.		
<b>Signature</b>	<b>Date</b>	

*DHMH 1770 BUILDING KEY REQUEST FORM, Version 1.0 (March 2015)*



## IX. Appendix F MDH Employee Offboarding Supervisor's Checklist

### Employee Offboarding

#### Supervisor's Checklist for Offboarding an Employee

##### Initial Actions Upon Receipt of Employee's Letter of Separation:

- Submit employee's letter of separation to Unit HR Liaison immediately (resignation, retirement, internal or external transfer). **Note:** This is *critical*, as the Unit HR Liaison is responsible for notifying the assigned HR Officer in the Office of Human Resources within 24 hours of the employee submitting the letter.

Within 24 hours of receiving the offboarding files from the Unit HR Liaison, provide the employee with:

- Completed *Employee Acknowledgement Memo* (which includes the Employee's Off-Boarding Obligations and, in all cases except internal transfer, the Employee Off-Boarding Information Sheet)

The employee must complete the obligations and return the initialed Memo to the supervisor. (The Information Sheet, if applicable, is for the employee's information and need not be returned.)

- Knowledge Transfer Plan*

The employee must complete the plan and return it to the supervisor; the employee and supervisor should meet to review the completed plan prior to the employee's departure.

The supervisor must return both employee's initialed Memo and the Supervisor's Offboarding Checklist to the Unit HR Liaison on the employee's last day on duty as verification that all offboarding tasks are complete.

##### Supervisor's Obligations Prior to Employee's Departure:

- Inventory employee's workspace.
- Confirm transfer of files, documents, emails, other records and voicemail passcode from employee to supervisor.
- Ensure that employee's pertinent documents, records and files are labeled and organized in hard copy form.
- Review with employee the completed Knowledge Transfer Plan for current projects, assignments, internal and external contacts and other key information.
- Notify team and appropriate stakeholders of employee's departure.
- Determine who assumes the departing employee's responsibilities.
- Cancel employee's signature/approval authority (if applicable).
- Confirm with employee that the following tasks have been completed:
  - All State-owned equipment has been relinquished (e.g., computer, mobile phone, calling cards, laptop, tablet, etc.)
  - All electronic files containing State data from personally owned computers, mobile devices, cloud storage and storage media have been migrated and deleted
  - All State-licensed software on personally owned computers and mobile devices has been uninstalled
  - All paper documents containing MDH data have been returned or destroyed
  - MDH has been given access and passwords for any electronic files being left at MDH
  - Web administrator(s) has been contacted to remove employee references from web content
  - Employee's keys and ID badge(s) have been turned in to the employee's supervisor (if applicable)
  - All parking permits and gas cards associated with State vehicles have been returned (if applicable)
  - Employee has removed all personal items from office or workspace
  - Any other applicable equipment and/or property has been returned

##### Supervisor's Obligations After Employee's Departure:

- Clear or change all passwords
- Check voicemail messages on employee's line and change message on voicemail
- Check calendars for appointments that should be cancelled or rescheduled
- Remove employee from recurring meetings
- Confirm building access and security cards have been deactivated (if applicable)

## X. Appendix G *Standard Operating Procedure for Requests for Protected Health Information*

<b>Maryland Department of Health Laboratories Administration 1770 Ashland Avenue Baltimore, Maryland 21205</b>  <b>Robert A. Myers, Ph.D., Director</b>	<b>Standard Operating Procedure  Requests for Protected Health Information  CLINICAL ONLY</b>	<b>Date Revised: 11/16/2017</b>  <b>Page: 1 of 3</b>
---	---	--

### 1. Mission and Purpose

The mission of the Laboratories Administration is to promote and preserve the health and well being of the people in Maryland from emerging and reemerging infectious diseases and other environmental hazards. The Laboratories Administration works in partnership with public and private agencies at the local, state and federal levels.

In accordance with the Annotated Code of Maryland, Health General Article, and federal HIPAA regulations, the following Standard Operating Procedure (SOP) has been established to ensure the legal sufficiency of requests for medical records. The following are established criteria for the legal review and release of records.

PIA (Public Information Act) requests are processed through the Laboratories Administration's Executive Office and should not be handled at the Divisional level.

Reasonable efforts to verify authorization should always be made and documented.

Release of medical results should be documented in Starlims.

### 2. Authorization for Release of Records

- A. The Laboratories Administration may disclose medical information with the authorization of the "person in interest" (patient or person authorized to consent to the health care for a minor or adult).
- B. The authorization must include the following information:
  - i. Be in writing, dated and signed by the person in interest;
  - ii. State the name of the health care provider;
  - iii. Identify the recipient of the information;
  - iv. Provide a description of the information to be disclosed;
  - v. Provide a description of the purpose for the disclosure;
  - vi. State the period of the time in which the authorization is valid, which may not exceed one year, except:
    - a. In cases involving criminal justice referrals which are valid until 30 days following the final disposition;
    - b. Where the person in interest is a resident of a nursing home in which case the authorization is valid until revoked.

<b>Maryland Department of Health Laboratories Administration 1770 Ashland Avenue Baltimore, Maryland 21205</b>  <b>Robert A. Myers, Ph.D., Director</b>	<b>Standard Operating Procedure</b>  <b>Requests for Protected Health Information</b>  <b>CLINICAL ONLY</b>	<b>Date Revised:</b> <b>11/16/2017</b>  <b>Page: 2 of 3</b>
---	---	--

- C. If the request for medical information pertains to a minor or an adult under supervision of a parent or guardian, search for the laboratory test results in Starlims to determine if parent(s) or guardian(s) can be verified.
- D. If parent(s) or guardian(s) cannot be verified, supporting documentation must be provided to establish “evidence of authority” to act on behalf of the minor or adult under supervision.
- E. Upon receipt of “evidence of authority,” test results may be released.
- F. Release of test results are documented in Starlims.
- G. All healthcare providers must be notified prior to releasing health information to a “person in interest.” Notification to healthcare providers can be forwarded via fax. Notification is not provided if the Laboratories Administration does not have a healthcare provider on record.
- H. The person in interest must be provided with a copy of the signed authorization.

### 3. Required Statements on Authorization

In addition to the above requirements, the authorization must also contain statements adequate to place the person in interest on notice of the following:

#### A. Revocation

- i. The right to revoke the authorization in writing (except in cases of criminal justice referrals);
- ii. A description of how to revoke the authorization;
- iii. The effective date of the revocation (date of receipt).

#### B. Prohibition on Conditioning of Authorization

- i. The Laboratories Administration is prohibited from conditioning the provision of treatment, payment, enrollment in a health plan or eligibility for benefits on the requirement that a person in interest sign the authorization.

#### C. Redisclosure

- i. The information disclosed may be subject to redisclosure (as set forth in #5 below).

<b>Maryland Department of Health Laboratories Administration 1770 Ashland Avenue Baltimore, Maryland 21205</b>  <b>Robert A. Myers, Ph.D., Director</b>	<b>Standard Operating Procedure</b>  <b>Requests for Protected Health Information</b>  <b>CLINICAL ONLY</b>	<b>Date Revised:</b> <b>11/16/2017</b>  <b>Page: 3 of 3</b>
---	---	--

#### 4. Disclosure to Medical Providers

- A. The Laboratories Administration may disclose medical record(s) without authorization to another healthcare provider for the sole purpose of treatment.
- B. Medical providers must provide their medical license number on the Request for Access to Records Form before medical information can be disclosed. Medical license number is entered into Starlims communication log.
  - i. Medical license number is an eleven (11) digit number.
- C. Records may be released to the provider's authorized employees, agents, medical staff, medical students, or consultants for the sole purpose of offering, providing, evaluating, or seeking payment for health care to patients or recipients by the provider.
- D. Records may also be released to another governmental agency (including the Office of the Medical Examiner) in an effort to assist these agencies with performing their government duties.


#### 5. Faxing Records to Medical Providers

Records may be forwarded to medical providers via fax if the provider has the following items below. Medical provider receipt does not need to be verified.

- A. A fax machine designated for receipt of medical records;
- B. Located in a secured area;
- C. Not accessible to the general public.

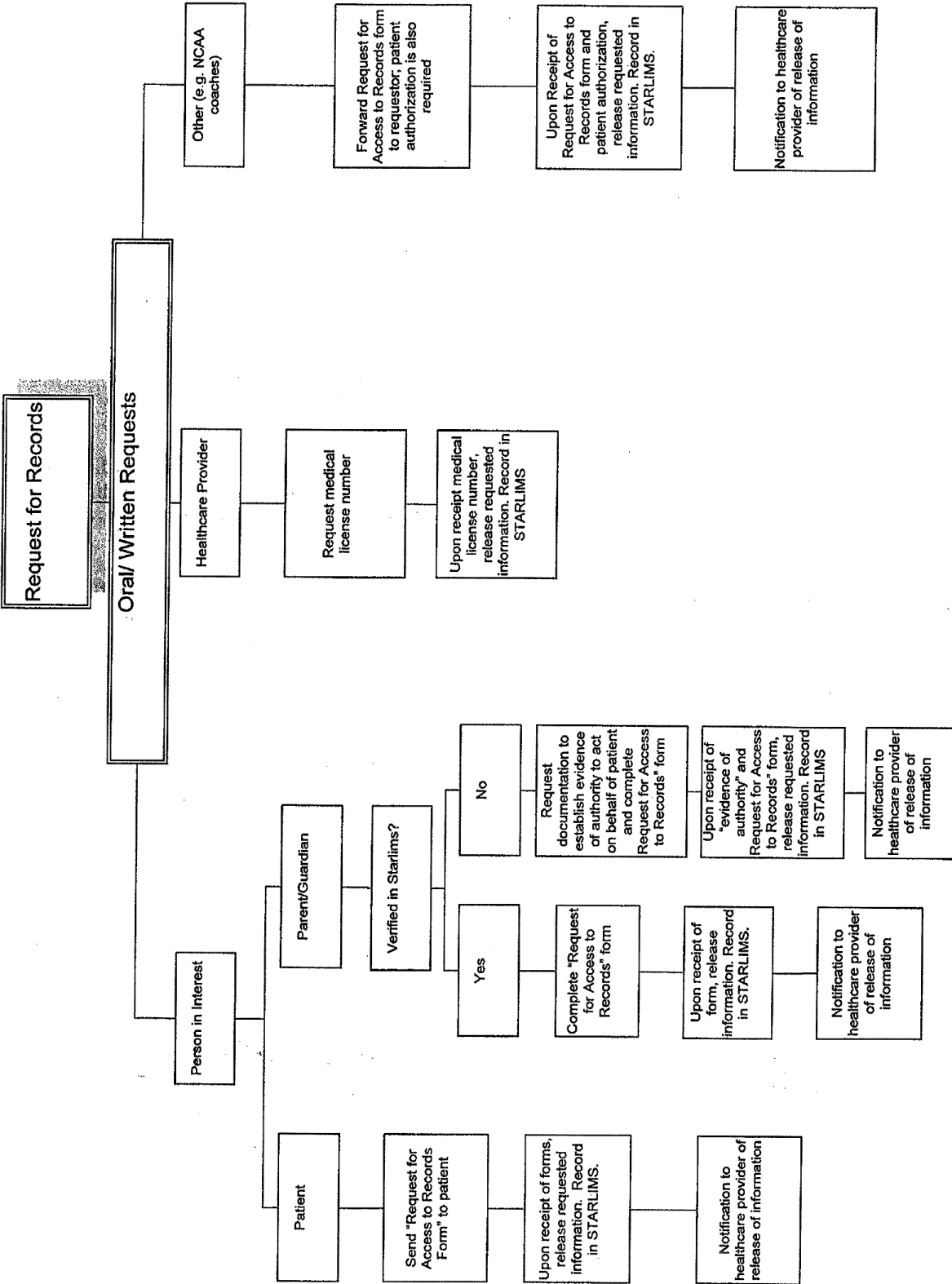
Note: If additional clarification is needed, please contact Administrator Renee Scurry at (443) 681-3805.

Approved:



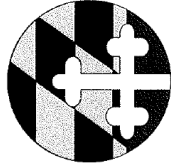
**Robert A. Myers, Ph.D.**  
**Director**

Effective Date: 11/16/17



XI. Appendix H Request for Protected Health Records Form

Request for Access to Records Form



MARYLAND Department of Health

Larry Hogan, Governor · Boyd Rutherford, Lt. Governor · Dennis Schrader, Secretary

Laboratories Administration Robert A. Myers, Ph.D., Director

Purpose: This form is used to confirm the direction of an individual to authorize MDH to request, to use, or to disclose the individual's health information.

Please type or print neatly; we are not able to process incomplete or illegible forms. \*Indicates mandatory fields

SECTION A: Identity of the Requestor of Individual's Health Information (Check One).

- Patient (Adult) Patient (Minor Consent) Parent of Minor Child Guardian of Minor Child Parent/Guardian authorized to consent to healthcare (Adult) OTHER

Requestor (Self): Phone:

Address: Fax: (Must be a secured fax machine)

SECTION B: Individual's Health Information Authorized for Use and Disclosure.

\*Last Name: \*First Name: MI: \*Date of Birth: \*Street Address: Apt #: \*City: \*State: \*Zip: Phone: (home) (work)

SECTION C: Disclosure Being Authorized.

1. Provide a detailed description of the health information you are authorizing us to disclose.

2. The purpose of the disclosure:

SECTION D: Expiration and Revocation.

(IF THIS SECTION IS NOT COMPLETED, THE LABORATORIES ADMINISTRATION CANNOT ACCEPT THIS FORM.)

Expiration: This authorization will expire one year from today's date unless otherwise noted (complete one):

- ONE YEAR FROM TODAY'S DATE: On occurrence of the following event (which must relate to the individual or to the purpose for which the disclosure has been authorized):

**Right to Revoke:** I understand that I may revoke this authorization at any time by giving written notice of my revocation to the Laboratories Administration. In order to obtain a revocation form to revoke this authorization, I understand that I may contact \_\_\_\_\_. I understand that revocation of this authorization will not affect any action that the Laboratories Administration or others named or unnamed took in reliance on this authorization before the Laboratories Administration received my written notice of revocation.

**SECTION E: Signature.**

**To the Individual – Please Read the Following:**

I authorize the disclosure of my health information as described in Sections C and D above. I understand this authorization is voluntary.

I understand that if the persons or organizations I authorize to receive and/or use my health information are not subject to the federal or state health information privacy laws, they might further disclose the health information, and it may no longer be protected by the health information privacy laws.

I have had full opportunity to read and consider the contents of this authorization, and I confirm that the contents are consistent with my intent.

**Signature:** \_\_\_\_\_ **Date:** \_\_\_\_/\_\_\_\_/\_\_\_\_

Medical License Number (if applicable) \_\_\_\_\_

If a personal representative is making this request, please attach a copy of any document granting legal authority and complete the following:

Personal Representative's Name: \_\_\_\_\_ **Date:** \_\_\_\_/\_\_\_\_/\_\_\_\_

Relationship to Individual: \_\_\_\_\_

---

Please return this form via fax to (443) 681-4501 or via email to [mdllabs.recordsrequest@maryland.gov](mailto:mdllabs.recordsrequest@maryland.gov)

*The Laboratories Administration is prohibited from conditioning the provision of treatment, payment, enrollment in a health plan or eligibility for benefits on the requirement that a person in interest sign the authorization.*

XII. Appendix I Revocation of Access to Records Form



**MARYLAND**  
**Department of Health**

Larry Hogan, Governor · Boyd Rutherford, Lt. Governor · Dennis Schrader, Secretary

Revocation of  
Request for Access to  
Records

Laboratories Administration  
Robert A. Myers, Ph.D., Director

**SECTION A: Individual's Information**

Last Name: \_\_\_\_\_ First Name: \_\_\_\_\_ MI: \_\_\_\_\_ Date of Birth: \_\_\_\_/\_\_\_\_/\_\_\_\_

Street Address: \_\_\_\_\_ Apt#: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

Phone: (home) \_\_\_\_\_ (work) \_\_\_\_\_

**Section B: Statement of Revocation**

I revoke my previous authorization to the Laboratories Administration for disclosure of my protected health information (PHI) as described below.

I understand that this revocation of my authorization will NOT affect any action that the Laboratories Administration or others took in reliance on my authorization before they received this written notice of my revocation.

I understand that re-disclosure of any information released prior to this revocation may have already occurred or may occur in the future without my knowledge or consent; therefore, the privacy of my PHI may no longer be protected by law.

**Section C: Description of Authorization Revoked**

- I hereby revoke any and all authorizations to the Laboratories Administration to release my PHI to any third party.
- I hereby revoke my authorization dated \_\_\_\_/\_\_\_\_/\_\_\_\_, which authorized the Laboratories Administration to release my PHI to: \_\_\_\_\_

**Section D: Individual's Signature**

Print Name: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

If this revocation is signed by a personal representative on behalf of the individual, complete the following:

Personal Representative's Name \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

Relationship to Individual: \_\_\_\_\_

Please return this form via fax to (443) 681-4501 or via email to [mdlabs.recordsrequest@maryland.gov](mailto:mdlabs.recordsrequest@maryland.gov)



**XIII.** Appendix J *Records Retention and Disposal Schedule*

<https://health.maryland.gov/laboratories/secure/Documents/Records%20Retention%20and%20Disposal%20Schedule.pdf>

**XIV.** Appendix K *1770 Tenant Handbook*

[https://health.maryland.gov/laboratories/docs/1770%20Tenant%20Handbook%20v1.3.1%2009-2017%20\(FINAL\).pdf](https://health.maryland.gov/laboratories/docs/1770%20Tenant%20Handbook%20v1.3.1%2009-2017%20(FINAL).pdf)

**XV. Appendix L Laboratories Administration Employee Temporary Keycard Authorization Form**

**Laboratories Administration Employee Temporary Keycard Authorization Form**

**The purpose of this form is to ensure the individual requesting a TEMP keycard is a current Laboratories Administration (LA) employee in good standing. The LA employee's divisional supervisor/manager/division chief, LA Personnel Officer, Safety Security Officer, or Quality Assurance Officer completing this form has verified to the best of their knowledge the individual requesting a TEMP keycard is an LA employee.**

EMPLOYEE NAME: \_\_\_\_\_

PHONE #: \_\_\_\_\_ DATE: \_\_\_\_\_

TEMP KEYCARD NUMBER: \_\_\_\_\_

**DIVISIONAL SUPERVISOR/MANAGER/DIVISION CHIEF, LA PERSONNEL OFFICER, SAFETY SECURITY OFFICER, or QUALITY ASSURANCE OFFICER APPROVAL**

PRINTED NAME: \_\_\_\_\_

SIGNATURE: \_\_\_\_\_

**Front Deck Security Officer on Duty:** \_\_\_\_\_

I UNDERSTAND AND ACKNOWLEDGE RECEIPT OF THE TEMP KEYCARD DESIGNATED ABOVE. I ALSO AGREE NOT TO LOAN, TRANSFER, GIVE POSSESSION OF, MISUSE, MODIFY OR ALTER THE ABOVE TEMP KEYCARD. I UNDERSTAND THE TEMP KEYCARD MUST BE RETURNED AT THE CLOSE OF BUSINESS ON THE DATE NOTED ABOVE. I AGREE THE USE OF THE TEMP CARD HAS BEEN ISSUED TO CONDUCT ONLY APPROVED LABORATORIES ADMINISTRATION BUSINESS. I UNDERSTAND AND AGREE THAT VIOLATION OF THIS AGREEMENT MAY RENDER ME RESPONSIBLE FOR ANY MONETARY DAMAGES OR OTHER EXPENSE, THAT ARE DIRECTLY OR INDIRECTLY A RESULT OF FAILURE TO RETURN THE ABOVE ISSUED TEMP KEYCARD. I ALSO UNDERSTAND AND AGREE THAT VIOLATION OF THIS AGREEMENT MAY RESULT IN FURTHER DISCIPLINARY ACTION BEING TAKEN AGAINST ME.

PERSON RECEIVING TEMP KEYCARD: \_\_\_\_\_  
(Print Name)

SIGNATURE/DATE RECEIVED ON: \_\_\_\_\_