10.10.11.00

Title 10 DEPARTMENT OF HEALTH AND MENTAL HYGIENE

Subtitle 10 LABORATORIES

Chapter 11 Biological Agents Registry Program

Authority: Health-General Article, §§17-601—17-605, Annotated Code of Maryland

10.10.11.01

.01 Purpose.

The purpose of this chapter is to help protect the people of Maryland against the potential threat of biological terrorism by establishing a program to register persons that possess, maintain, transfer, or receive biological agents in the State.

10.10.11.02

.02 Scope.

A. This chapter contains the standards and requirements a person that possesses, maintains, transfers, or receives a biological agent in this State shall meet to comply with the registration of biological agents.

B. This chapter does not apply to a biological agent or a certified laboratory or facility that is exempt from the requirements for the interstate shipment of etiologic agents under 42 CFR §§73.5 and 73.6, 9 CFR §§121.5 and 121.6, and 7 CFR §331.5.

10.10.11.03

.03 Definitions.

A. In this chapter, the following terms have the meanings indicated.

B. Terms Defined.

(1) "Access" means the ability or the means necessary to:

(a) Read, write, modify, or communicate BAR information; or

(b) Otherwise make use of any system resource related to BAR information.

(2) "Access control" means a method of restricting access to a BAR information resource, allowing only an authorized individual access to the resource.

(3) "Authentication" means the corroboration that a person is the one claimed.

(4) “BAR” means the Department’s Biological Agents Registry.

(5) BAR Information.

(a) "BAR information" means information submitted to the BAR Program by a person required to report a biological agent under this chapter.

(b) "BAR information" identifies:

(i) A person in this State who possesses, maintains, transfers, or receives a biological agent; and

(ii) The biological agents possessed, maintained, transferred, and received by a person in this State.

(c) "BAR information" includes:

(i) Information contained in any of the documents and records that the BAR Program collects, requests, maintains, processes, or stores;

(ii) Information released by the BAR Program, a trusted partner, or a BAR information custodian; and

(iii) Biological agent incident response plans submitted to a local jurisdiction as required by this chapter.

(6) BAR Information Custodian.

(a) "BAR information custodian" means an individual designated by a trusted partner and authorized by the Department in a trusted partner agreement to receive and maintain BAR information.

(b) "BAR information custodian" may include:

(i) A health officer;

(ii) An Emergency Management Director or equivalent; and

(iii) Other alternately designated and authorized individuals with a legitimate need to know the BAR information as it relates to the performance of the person's duties.

(7) "BAR Program" means the Department’s BAR Program within the Laboratories Administration’s Office of Laboratory Emergency Preparedness and Response.

(8) "Biological agent" means:

(a) A select agent or toxin listed in 42 CFR §§73.3 and 73.4, 7 CFR §331.3, and 9 CFR §§121.3 and 121.4;

(b) A genetically modified microorganism or genetic element from an organism listed in 42 CFR §§73.3 and 73.4, 7 CFR §331.3, and 9 CFR §§121.3 and 121.4, shown to produce or encode for a factor associated with disease; or

(c) A genetically modified microorganism or genetic element that contains nucleic acid sequences coding for a toxin listed in 42 CFR §§73.3 and 73.4, and 9 CFR §§121.3 and 121.4, or the toxin's subunits.

(9) Biological Agent Incident.

(a) "Biological agent incident" means a breach of containment or imminent threat of a breach of containment of a biological agent that poses an immediate threat to an individual's health and safety.

(b) "Biological agent incident" includes any situation that may cause or potentially cause an exposure to or release of a biological agent, as set forth in Regulation .12B of this chapter.

(10) "Biosafety Level (BSL)" means the level of work practices, facility design, and safety equipment to prevent transmission of biologic agents to workers, other individuals, and the environment, as defined in the BMBL.

(11) "Biosafety Level-2 (BSL-2)" means the BSL used when:

(a) Work is done with biological agents associated with human disease; and

(b) The route of transmission is by:

(i) Percutaneous injury;

(ii) Ingestion; or

(iii) Mucous membrane exposure.

(12) "Biosafety Level-3 (BSL-3)" means the BSL used when:

(a) Work is done with indigenous or exotic agents associated with a potentially serious or lethal human disease; and

(b) The route of transmission is aerosol inhalation.

(13) Biosafety Level-4 (BSL-4).

(a) "BSL-4" means the BSL used when work is done with a dangerous and exotic biological agent that poses a high risk of life-threatening or lethal human disease that:

(i) May be transmitted via the aerosol route;

(ii) Has an unknown mode of transmission; or

(iii) Has no available vaccine or therapy.

(b) "BSL-4" includes the BSL used when the agent has a close or identical antigenic relationship to BSL-4 agents.

(14) “BMBL” means the “Biosafety in Microbiological and Biomedical Laboratories”, which is incorporated by reference in Regulation .04 of this chapter.

(15) "Centers for Disease Control and Prevention (CDC)" means the federal Centers for Disease Control and Prevention of the federal Department of Health and Human Services.

(16) "Compact Disc-Recordable (CD-R)" means a type of write once, read many compact disc format that allows one-time recording of digital information on the disc.

(17) Contingency Plan.

(a) "Contingency plan" means a plan for responding to an information system emergency.

(b) "Contingency plan" includes:

(i) Installing system information from backups;

(ii) Preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency; and

(iii) Recovering from a disaster.

(18) "Decryption" means reversing the protective encryption algorithm process to make the previously unintelligible plaintext available for further processing as intelligible plaintext.

(19) "Deficiency" means a documented lack of compliance with a standard or requirement of the BAR Program set forth in this chapter.

(20) "Department" means the Department of Health and Mental Hygiene.

(21) "Emergency management director" means an individual appointed by the Governor of Maryland, who is directly responsible for the organization, administration, and operation of the local organization for emergency management in the local jurisdiction as set forth in Public Safety Article, §14-109, Annotated Code of Maryland.

(22) Encryption.

(a) "Encryption" means transforming confidential plaintext into ciphertext to protect it so that the data can be securely stored.

(b) "Encryption" includes encrypting with an algorithm that combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible.

(23) "Etiologic" means disease causing.

(24) "Facility" means a building or complex of buildings owned by the same person and located at a single mailing address.

(25) "Genetic element" means a nucleic acid sequence shown to produce or encode for a factor associated with a disease, a toxin, or a toxin's subunits.

(26) "Local jurisdiction" means a county of the State or Baltimore City.

(27) "Maintaining a biological agent" means manipulating or holding a biological agent to sustain or enhance viability, infectivity, or toxicity.

(28) "Maryland Institute for Emergency Medical Services Systems (MIEMSS)" means the unit established by Education Article, §13-503, Annotated Code of Maryland.

(29) "MDE" means the Maryland Department of the Environment.

(30) "MEMA" means the Maryland Emergency Management Agency.

(31) Nature of a Biological Agent.

(a) "Nature of a biological agent" means the term that describes the kind or type of material or organism the agent is.

(b) "Nature of a biological agent" includes:

(i) Toxin;

(ii) Bacterium;

(iii) Virus;

(iv) Rickettsia;

(v) Fungus;

(vi) Allergen;

(vii) Genetic element; or

(viii) Any combination of §B(30)(b)(i)—(vii) of this regulation.

(c) "Nature of a biological agent" does not include the name or identity of the biological agent.

(32) Person.

(a) "Person" means an individual, receiver, trustee, guardian, personal representative, fiduciary, or representative of any kind and any partnership, firm, association, corporation, or other entity.

(b) "Person" includes State and federal units of government.

(33) "Personal identification number (PIN)" means a number or code assigned to an individual and used to provide verification of identity.

(34) Personal Protective Equipment (PPE).

(a) "Personal protective equipment (PPE)" means the type of physical barrier equipment necessary to:

(i) Protect an individual from contact with a biological agent; or

(ii) Prevent transmission of a biological agent.

(b) "Personal protective equipment (PPE)" includes, but is not limited to:

(i) Face protection, such as a face shield or goggles;

(ii) Protective clothing, such as a laboratory coat or gloves; and

(iii) Respiratory protection, such as a surgical mask, respirator, or self-contained breathing apparatus.

(c) "Personal protective equipment (PPE)" includes:

(i) For BSL-2, laboratory coat, gloves, and face protection as needed;

(ii) For BSL-3, protective laboratory clothing, gloves, booties, hair covering, face protection, and respiratory protection as needed; and

(iii) For BSL-4, full body, air-supplied, positive pressure personnel suit.

(35) "Possessing a biological agent" means handling, holding, maintaining, owning, or storing a biological agent within the State.

(36) Responsible Official.

(a) "Responsible official" means an individual designated by a person required to report under this chapter to act on the person's behalf.

(b) "Responsible official" includes an individual designated as an alternate responsible official who acts in the responsible official's absence.

(37) "Role-based access" means a security mechanism for granting user access to a computer information system containing BAR information, based upon the user's job function.

(38) "Security incident" means a situation when BAR information is:

(a) Intentionally or unintentionally released to an unauthorized person; or

(b) Otherwise compromised in a way that allows unauthorized access.

(39) Security Self-Assessment.

(a) "Security self-assessment" means a person's formal assessment of the sensitivity, vulnerabilities, and security of the person's operations and programs related to the BAR information the person receives, manipulates, stores, or transmits.

(b) "Security self-assessment" includes the:

(i) Procedures and processes for determining a person's compliance with the BAR information security standards in this chapter;

(ii) Documentation certifying to the BAR Program that a person meets the BAR information security standards;

(iii) Identification and management of security risks; and

(iv) Security standards self-assessment check list provided by the BAR Program.

(40) "Technical security measure" means a process that is put in place to protect information and control individual access to information in order to guard data integrity, confidentiality, and availability.

(41) "Token" means an electronic device for authenticating user identification and allowing access to a door or computer information system.

(42) Toxin.

(a) "Toxin" means a biologically active poisonous substance that is:

(i) Produced by a living cell or an organism; and

(ii) Harmful to another organism.

(b) "Toxin" does not include:

(i) A poisonous substance produced by a living organism for medical purposes, inactivated for use as a vaccine; or

(ii) A toxin preparation for biomedical research use at a lethal dose of 50 percent (LD50) for vertebrates of more than 100 nanograms per kilogram body weight.

(43) "Transfer" means the physical relocation of a biological agent from one facility or person to another.

(44) Trusted Partner.

(a) "Trusted partner" means a person with whom the Department has a valid trusted partner agreement to receive, possess, maintain, and transfer or share BAR information, as set forth in this chapter.

(b) "Trusted partner" includes only MDE, MEMA, MIEMSS, and a local jurisdiction where a biological agent is located.

(45) Trusted Partner Agreement.

(a) "Trusted partner agreement" means a document describing the arrangement between the Department and a trusted partner regarding how, when, and to whom information is released from the BAR.

(b) "Trusted partner agreement" includes the documentation that describes all the policies, procedures, and mechanisms agreed upon to protect the integrity, confidentiality, and availability of BAR information.

(46) "User-based access" means a security mechanism used to grant system access to users, based upon the identity of the user.

.04 Incorporation by Reference.

A. In this chapter, the following documents are incorporated by reference.

B. Documents Incorporated.

(1) 29 CFR §1910.1450, as amended.

(2) 42 CFR 73, as amended.

(3) 9 CFR 121, as amended.

(4) 7 CFR 331, as amended.

(5) CDC/NIH publication, “Biosafety in Microbiological and Biomedical Laboratories”, 5th Edition, December 2009.

10.10.11.05

.05 Registering Under the Biological Agents Registry Program.

A person in the State shall participate in and comply with the State's BAR Program by registering with and reporting to the Department, in the manner set forth in this chapter, the information required by the Department.

10.10.11.06

.06 Compliance with Federal Standards.

A person that possesses, maintains, transfers, or receives a biological agent shall comply with all safeguards contained in 42 CFR 73, 9 CFR 121, and 7 CFR 331 that apply to a person registered to transfer the same agent under federal law and regulation.

10.10.11.07

.07 Responsibilities of the Department.

The Department shall:

A. Establish and maintain a registry that identifies the biological agents possessed, maintained, transferred, and received by a person in this State;

B. Conduct facility surveys by mail, by on-site visit, or both, initially and periodically after that, to:

(1) Ensure compliance with the standards and requirements of the BAR Program; and

(2) Address any deficiencies or complaints;

C. Provide or approve the forms that a person shall complete and submit to the Department under the BAR Program;

D. Issue notice when a survey of a facility yields findings of deficiencies related to the standards or requirements of the BAR Program;

E. Investigate a complaint that a facility or an employee is not complying with the standards or requirements of the BAR Program; and

F. Release BAR information, as provided in this chapter, to:

(1) State and federal law enforcement agencies;

(2) CDC; and

(3) Trusted partners.

10.10.11.08

.08 Responsible Official; Alternate Responsible Official.

A. A person required to report to the BAR Program under this chapter shall designate an individual to be the responsible official who:

(1) Is familiar with the requirements of this chapter;

(2) Has the authority and responsibility to act on the person's behalf related to a biological agent; and

(3) Shall ensure compliance with the requirements of this chapter.

B. The responsible person shall ensure that the annual inspection and specific reporting requirements and mechanisms are carried out in accordance with 42 CFR §73.9.

C. A person required to report to the BAR Program under this chapter shall:

(1) Designate one or more individuals to be an alternate responsible official to act in the responsible official's absence; and

(2) Ensure that the individual designated as an alternate responsible official has the authority required in §A of this regulation to ensure compliance with this chapter when acting in the responsible official's absence.

10.10.11.09

.09 Reporting Requirements.

A. What to Report. Using reporting forms provided or approved by the Department, a person shall:

(1) Identify all non-exempt biological agents that the person possesses, maintains, transfers, or receives listed under:

(a) Select agents and toxins in:

(i) 42 CFR §73.3;

(ii) 9 CFR §121.3; and

(iii) 7 CFR §331.3; and

(b) Overlap select agents and toxins in:

(i) 42 CFR §73.4; and

(ii) 9 CFR §121.4;

(2) Indicate as part of the identification if a biological agent is:

(a) Viable or nonviable;

(b) Purified genomic material;

(c) Recombinant DNA;

(d) Used in small or large animal work;

(e) Used in large-scale production; and

(f) A toxin;

(3) Identify the physical location of a laboratory and storage area within a facility where a biological agent is contained;

(4) Identify the biosafety level required for the biological agent; and

(5) Identify the individual in charge of the biological agent and information needed to contact that individual.

B. When to Report. A person shall:

(1) Complete and submit a report within 30 days of receiving:

(a) An initial request to report from the Department; and

(b) A periodic request to report from the Department;

(2) Submit a report of each transfer and receipt of a biological agent within 24 hours of completing a transfer as set forth in Regulation .10D of this chapter;

(3) Respond in writing to a deficiency notice from the Department within 10 work days of receiving the notice; and

(4) Respond in writing to notice of a complaint within 10 work days of receiving notice from the Department.

C. Who Submits Reports. A person shall submit a report dated and signed by the:

(1) Individual who actually possesses, maintains, transfers, or receives and has charge of a biological agent; and

(2) Responsible official of the facility where the biological agent is located.

D. Where to Report. A person shall return all completed reports and other correspondence to the BAR Program, c/o Laboratories Administration, Department of Health and Mental Hygiene.

10.10.11.10

.10 Additional Requirements Covering Possession, Maintenance, Transfer, or Receipt of a Biological Agent.

A person possessing, maintaining, transferring, or receiving a biological agent at a facility located in the State shall:

A. Possess a laboratory and personnel equipped and capable of handling the biological agents at BSL 2, 3, or 4, depending on the agent and the type of work being performed with the agent, as contained in the BMBL;

B. Meet specific requirements for handling a toxin subject to this chapter as set forth in 29 CFR §1910.1450;

C. Allow an official representative of the Department to determine compliance with the standards and requirements of this chapter by:

(1) Conducting an on-site inspection of the person's facility, including all:

(a) Storage areas;

(b) Laboratories; and

(c) Operations; and

(2) Examining and reviewing procedures and documentation related to biological agents;

D. Submit a copy of each completed CDC form documenting transfer or receipt of a biological agent, within 24 hours of completing a transfer or receipt, to the BAR Program; and

E. Inform the Emergency Management Director in the local jurisdiction where the biological agent is located of the nature and facility location of each reported biological agent that is located in that jurisdiction.

10.10.11.11

.11 Reporting of Unauthorized Activities.

On learning that there is an unauthorized activity involving a biological agent, including the unauthorized possession, unauthorized attempted possession, unauthorized maintenance, unauthorized transfer, or unauthorized receipt of a biological agent, a person shall immediately alert the Department by:

A. Telephoning the:

(1) Laboratories Administration at 410-767-6100 between 8 a.m. and 4:30 p.m. weekdays; or

(2) Department's emergency after-hours and weekend telephone line at MIEMSS at 410-795-7365 at other times;

B. Asking the individual taking the call to direct the information being reported to the BAR Program or the Director of the Laboratories Administration; and

C. Reporting details about the unauthorized activity set forth in this regulation, such as:

(1) The location of a facility and laboratory involved;

(2) The identity of a person possessing or attempting to possess a biological agent; and

(3) Other details pertinent to the report.

10.10.11.12

.12 Biological Agent Incident Response Plan.

A. Requirement. A person required to report under this chapter shall:

(1) Develop, implement, and maintain a written biological agent incident response plan;

(2) Review the plan annually and revise the plan as necessary; and

(3) Submit a copy of the plan and any amendments to the plan to the:

(a) Emergency management director in the local jurisdiction where the biological agent is located; and

(b) BAR Program.

B. A person required to submit a biological agent incident response plan shall:

(1) Coordinate the biological agent incident response plan with any facility-wide plans;

(2) Keep the biological agent incident response plan current to reflect actual procedures and practices;

(3) Locate and maintain the biological agent incident response plan in the workplace;

(4) Make the biological agent incident response plan available to employees;

(5) Ensure that the biological agent incident response plan fully describes the response procedures for:

(a) The theft, loss, or release of a biological agent;

(b) Inventory discrepancies;

(c) Security breaches, including in computer information systems;

(d) Severe weather and other natural disasters;

(e) Workplace violence;

(f) Bomb threats;

(g) Suspicious packages;

(h) Emergencies such as:

(i) Fire;

(ii) Gas leaks;

(iii) Explosions; and

(iv) Power outages;

(i) Use of PPE;

(j) Use of onsite emergency equipment to protect both the facility and personnel;

(k) Employees to follow when performing:

(i) Rescue or medical duties;

(ii) Emergency medical treatment; and

(iii) First aid;

(l) Emergency evacuation, including:

(i) Type of evacuation;

(ii) Exit route assignments;

(iii) Safe distances; and

(iv) Places of refuge;

(m) Decontamination; and

(n) Site security and control;

(6) Ensure that the plan includes procedures that explain the:

(a) Risks and hazards associated with any biological agent on the premises; and

(b) Actions to contain the biological agent;

(7) Ensure that the plan contains the following information:

(a) The name and contact information for home, work, and emergencies, for the:

(i) Responsible official; and

(ii) Alternate responsible official;

(b) Where applicable, the name and contact information for:

(i) The building owner and manager;

(ii) Tenants; and

(iii) The official in charge of the building's physical security;

(c) Personnel roles and lines of authority and communication;

(d) Planning and coordination with local emergency responders; and

(e) A list of the PPE available and where the PPE is located in the facility;

(8) Conduct drills or exercises at least annually to test and evaluate the effectiveness of the plan;

(9) Notify the emergency management director in the local jurisdiction where the biological agent is located and the BAR Program:

(a) Before a drill or exercise is conducted; and

(b) When a biological agent incident has occurred;

(10) Prepare a report of the results of a drill, exercise, or biological agent incident;

(11) Review a report of the results of a drill, exercise, or biological incident to determine if the plan requires revision; and

(12) Within 10 days after a drill, exercise, or biological agent incident, submit a copy of the report to the:

(a) Emergency management director in the local jurisdiction where the biological agent is located; and

(b) BAR Program.

C. Monitoring Compliance. When a person submits a biological agent incident response plan to the BAR Program, the BAR Program shall:

(1) Review the plan for compliance with this chapter; and

(2) Verify that the person submitting the plan has provided the information for planning and coordinating with local emergency responders to the emergency management director in the local jurisdiction where the biological agent is located.

10.10.11.13

.13 BAR Information Confidentiality and Release of BAR Information.

A. Except as otherwise provided in this chapter, a person shall keep information prepared for or maintained in the BAR, including biological agent incident response plans required by Regulation .12 of this chapter:

(1) Confidential; and

(2) Protected from unauthorized access and use.

B. BAR information is not subject to State Government Article, Title 10, Subtitle 6, Annotated Code of Maryland.

C. Release or sharing of BAR information as authorized in this chapter does not render the BAR information released or shared a public record.

D. Except as provided in §§G—I of this regulation, a person to whom BAR information has been released may not release the information to another person unless the release is approved by the BAR Program.

E. The BAR Program may release BAR information only to:

(1) State and federal law enforcement agencies;

(2) CDC; and

(3) BAR information custodians of trusted partners.

F. Before the BAR Program releases BAR information to a person, except State and federal law enforcement agencies and the CDC, the person shall:

(1) Enter into and maintain a trusted partner agreement;

(2) Conduct a BAR information security self-assessment; and

(3) Submit the results of a BAR information security self-assessment to the BAR Program for approval.

G. Mutual Aid Response. When multiple local jurisdictions respond to an emergency, the emergency management director of one responding jurisdiction may share BAR information with an emergency management director from another local jurisdiction that is providing mutual aid by assisting with the emergency response.

H. Emergency Release Activation Process.

(1) A trusted partner may release on an emergency basis BAR information about the nature and location of a biological agent to another trusted partner or emergency public safety personnel when:

(a) An on-site alarm goes off at a person's facility where a biological agent is located and an individual at the site is required to place a telephone call to a 9-1-1 center;

(b) A 9-1-1 center dispatches emergency public safety personnel to a site where a biological agent is known to be located; or

(c) There is a reported breach of containment or imminent threat of a breach of containment of a biological agent that poses an immediate threat to the health and safety of the public or emergency public safety first responders.

(2) MIEMSS may release on an emergency basis the nature and location of a biological agent to a:

(a) Police officer, as defined in Public Safety Article, §3-201(e), Annotated Code of Maryland, who is responding to an emergency; and

(b) Fire, rescue, or emergency medical services entity, as defined in Public Safety Article, §7-101, Annotated Code of Maryland, when responding to an emergency.

I. 24/7 Access to BAR Information.

(1) MDE, MEMA, and MIEMSS may act as a back-up to the BAR Program by maintaining:

(a) 24/7 (24 hours a day, 7 days a week) access to BAR information; and

(b) Access to BAR information when a trusted partner:

(i) Experiences a BAR information computer information system malfunction; or

(ii) Otherwise does not have access to BAR information.

(2) MDE, MEMA, or MIEMSS may release BAR information regarding the nature and location of a biological agent to each other or another BAR Program trusted partner if the trusted partner:

(a) Has a computer information system failure or other incident that prevents access to BAR information; or

(b) Is unable to obtain access to BAR information.

J. Emergency Release of Name or Identity of a Biological Agent. MDE, MEMA, or MIEMSS may release by any necessary means of communication the name or identity of the specific biological agent located at the site of an emergency response to protect the health and safety of the public and emergency response personnel if:

(1) There is a breach in containment of a biological agent or there is an imminent threat of a breach of containment;

(2) The breach or imminent threat of a breach is confirmed by the:

(a) Responsible official; or

(b) Emergency public safety personnel at the scene of the emergency response; and

(3) The release is approved by the Department's physician on-call.

K. Departmental Authorization to Release Name or Identity of Biological Agent.

(1) The Department's physician on-call may release the name or identity of a biological agent as required to mitigate the risk and treat those exposed based on the potential threat to the health and safety of the public.

(2) The Department's physician on-call shall decide when, how, and to whom to release the name or identity of the biological agent.

L. Notification Protocol.

(1) When there is a breach or imminent threat of a breach in containment of a biological agent as described in §J of this regulation, the:

(a) Public safety personnel responding to an emergency shall contact the public safety personnel's 9-1-1 center; and

(b) 9-1-1 center personnel shall notify MIEMSS and each of the following individuals in the jurisdiction where the breach occurred:

(i) The emergency management director; and

(ii) The health officer.

(2) When MIEMSS receives notice of a breach or an imminent threat of a breach of containment of a biological agent, MIEMSS shall notify:

(a) The Department's:

(i) Physician on-call; and

(ii) BAR Program within the Office of Laboratory Emergency Preparedness and Response;

(b) MDE; and

(c) MEMA.

(3) Immediately after the Health Officer is notified by 9-1-1 center personnel, the health officer shall contact the Department's physician on-call to:

(a) Verify the BAR information release; and

(b) Confirm a plan of action regarding:

(i) Release of BAR information; and

(ii) Measures to be taken to protect the health and safety of the public.

M. Using a form provided by the BAR Program, a trusted partner shall notify the BAR Program within 72 hours after the:

(1) Trusted partner's BAR information custodian releases or shares BAR information; or

(2) Trusted partner releases or shares BAR information with another trusted partner.

10.10.11.14

.14 Method of Non-Emergency Release of BAR Information.

A. A person shall release and transfer BAR information to a trusted partner and a BAR information custodian in a secure manner, which includes the use of:

(1) Read-only optical or electronic media;

(2) Encryption and decryption; and

(3) Copy protection to prevent unauthorized copying or duplication.

B. Unless authorized or required by federal regulation as set forth in Regulation .04B(2)—(4) of this chapter and except as provided in Regulation .13G, H, J, and K of this chapter, a person other than the BAR Program may not release, transfer, or share BAR information using:

(1) A telephone;

(2) Voice mail;

(3) An electronic or mechanical recording device;

(4) An internet communication system, such as voice-over-internet-protocol (VoIP).

C. Release of BAR Information to a Local Jurisdiction, MDE, MEMA, and MIEMSS.

(1) The BAR Program shall release BAR information to a BAR information custodian of a local jurisdiction, MDE, MEMA, and MIEMSS:

(a) When notified by the BAR Program that the BAR information is available for release;

(b) In person;

(c) At the BAR Program office; and

(d) On weekdays between the hours of 8:30 a.m. and 3:30 p.m.

(2) A designated representative of the BAR Program shall provide a CD-R containing BAR information to a BAR information custodian of a local jurisdiction, MDE, MEMA, and MIEMSS after the BAR information custodian presents:

(a) A government issued photo identification, such as:

(i) A valid Maryland driver's license; or

(ii) An employee identification badge; and

(b) A prior CD-R containing BAR information, if the BAR Program's BAR information release log indicates a CD-R was provided at an earlier time.

D. BAR Program staff shall document the release of all BAR information to trusted partners in a permanent record that contains the:

(1) Name of the BAR information custodian;

(2) Identity of the trusted partner;

(3) Coded identity of the CD-R containing BAR information; and

(4) Date and time of the release or delivery of the CD-R.

10.10.11.15

.15 Release of BAR Information to Law Enforcement Agencies and CDC.

The BAR Program may release BAR information to State and federal law enforcement agencies and the CDC without a trusted partner agreement if the release of BAR information is pursuant to:

A. A communicable disease investigation commenced or conducted by:

(1) The Department; or

(2) A State or federal law enforcement agency having investigative authority; or

B. An investigation involving a release, theft, or loss of a biological agent.

10.10.11.16

.16 Release of BAR Information to Local Jurisdictions.

A. The Department shall release to a local jurisdiction the BAR information listed in §C of this regulation for each biological agent located within the local jurisdiction, if the local jurisdiction:

(1) Enters into and maintains a trusted partner agreement with the Department; and

(2) Limits the number of BAR information custodians in the local jurisdiction to the:

(a) Health officer or the health officer's designee; and

(b) Emergency management director or the emergency management director's designee.

B. The local jurisdiction may use the BAR information for:

(1) Protecting emergency first-responders, including:

(a) Fire fighters;

(b) Police officers; and

(c) Emergency employees, including:

(i) Emergency medical personnel;

(ii) Rescue workers; and

(iii) Public health emergency responders;

(2) Planning for emergency protection of the public related to the:

(a) Release of a biological agent; or

(b) Prevention of a release of a biological agent; and

(3) Conducting investigations related to biological agents.

C. Information Released. The BAR Program shall inform the BAR information custodian in the local jurisdiction of the:

(1) Location in the local jurisdiction of the biological agent, including the:

(a) Facility or entity name; and

(b) Physical address of the facility;

(2) Nature of each biological agent; and

(3) The BSL or PPE necessary to protect emergency responders from contact with or transmission of the biological agent.

10.10.11.17

.17 Release of BAR Information to MDE, MEMA, and MIEMSS.

The Department shall:

A. Release separately to the BAR information custodians of MDE, MEMA, and MIEMSS the BAR information listed in §C of this regulation for each biological agent located within the State, if MDE, MEMA, and MIEMSS each separately becomes a trusted partner by:

(1) Entering and maintaining a trusted partner agreement with the Department; and

(2) Authorizing and identifying the individual who is the designated BAR information custodian in the trusted partner agreement;

B. Make BAR information available to MDE, MEMA, and MIEMSS for the purpose of planning for the protection of the public related to the:

(1) Release of a biological agent, such as a breach in containment;

(2) Prevention of a release of a biological agent; and

(3) Mitigation and planning for the protection of:

(a) Critical infrastructure;

(b) Key assets; and

(c) Emergency public safety personnel; and

C. Provide the following BAR information of each biological agent in the State that is registered under this chapter to the BAR information custodian of MDE, MEMA, and MIEMSS, including for the entity that possesses, maintains, transfers, or receives a biological agent:

(1) Name and contact information of:

(a) The responsible official;

(b) The alternate responsible official; and

(c) Other personnel or staff listed by the facility who are responsible for a biological agent;

(2) Location of the biological agent, including the:

(a) Facility or entity name; and

(b) Physical address of the facility;

(3) Name or identity of each biological agent;

(4) Nature of each biological agent;

(5) BSL necessary to handle safely and contain the biological agent; and

(6) PPE necessary to protect emergency responders from contact with or transmission of the biological agent.

10.10.11.18

.18 BAR Information Updates.

The Department shall provide updated BAR information to the BAR information custodians of all trusted partners authorized under this chapter:

A. Within 30 days when there is an:

(1) Upward change in the BSL at a listed person's facility, for example from BSL-3 to BSL-4; or

(2) Addition to the BAR, including a new:

(a) Person possessing or maintaining a biological agent;

(b) Facility where a biological agent is located; or

(c) Biological agent; and

B. At least once each year.

10.10.11.19

.19 BAR Information Security Standards — General.

A. A trusted partner shall protect and maintain BAR information in a secure manner by limiting access only to a BAR information custodian who is:

(1) An individual designated by the trusted partner; and

(2) Authorized by the Department in a trusted partner agreement.

B. Before the Department shares BAR information with a trusted partner, the trusted partner shall:

(1) Develop, implement, and maintain administrative, physical, and technical security measures and practices to protect and safeguard the integrity, confidentiality, and availability of BAR information by managing and supervising the:

(a) Selection, execution, and use of security measures to protect BAR information; and

(b) Conduct of personnel in relation to the protection of BAR information;

(2) Assess potential risks and vulnerabilities to the BAR information in its possession using a BAR information security self-assessment checklist provided by the BAR Program; and

(3) Submit a:

(a) Completed BAR information security self-assessment; and

(b) Document verifying that the trusted partner's BAR information custodian has successfully undergone a security risk assessment as described in 42 CFR §73.7.

C. If a BAR information custodian believes that the security of BAR information has been or is suspected to have been misused, mishandled, lost, stolen, or otherwise compromised, the BAR information custodian shall immediately notify the:

(1) BAR Program; and

(2) Individuals who signed the BAR information custodian's trusted partner agreement.

10.10.11.20

.20 BAR Information Security Standards — Administrative Procedures.

A trusted partner shall establish and maintain administrative procedures to protect BAR information integrity, confidentiality, and availability, which include:

A. Entering and maintaining with the Department a trusted partner agreement that certifies that the trusted partner shall:

(1) Establish and implement the policies and procedures to carry out the requirements of this chapter; and

(2) Designate a BAR information custodian;

B. Establishing and implementing a contingency plan for protecting confidentiality of and access to BAR information when responding to a disaster or computer information system emergency, which includes:

(1) Preparing critical facilities that can be used to facilitate continuing protection of BAR information in the event of an emergency;

(2) Disaster recovery procedures to follow in the event of:

(a) Fire;

(b) Vandalism;

(c) Natural disaster; or

(d) Computer information system failure;

(3) An emergency mode operation plan that includes procedures for assuring continuing protection of BAR information when the trusted partner continues to operate in the event of:

(a) Fire;

(b) Vandalism;

(c) Natural disaster; or

(d) Computer information system failure; and

(4) Testing and revising procedures that document the process of periodically testing the written contingency plan procedures to determine:

(a) Weaknesses; and

(b) The subsequent process of revising the procedures, if necessary;

C. A mechanism for the receipt, viewing, manipulation, storage, release, dissemination, and disposal of BAR information;

D. Information-use policies that ensure that BAR information is used only as specified in this chapter;

E. Internal audit procedures for:

(1) Maintaining records of computer information system activity including:

(a) Logons;

(b) File accesses; and

(c) Security incidents; and

(2) Reviewing the records of computer information system activity for:

(a) Breaches in security; and

(b) Unauthorized access;

F. Personnel security procedures that ensure that only personnel who have the required authorizations and agency clearances have access to BAR information by:

(1) Providing oversight of unauthorized personnel when the personnel are performing their duties near BAR information, which includes:

(a) Supervision of maintenance personnel by an authorized and knowledgeable individual; and

(b) Assuring that unauthorized or unsupervised operating and maintenance personnel do not have and cannot acquire access to BAR information;

(2) Maintaining and reviewing a record of access authorizations that documents the levels of access granted to an individual accessing BAR information;

(3) Establishing personnel clearance procedures as a protective measure applied to determine that an individual's access to BAR information is permissible; and

(4) Ensuring that BAR information computer information system users, including maintenance personnel, receive security awareness training;

G. Employee termination procedures for ending an employee's employment or a user's access to BAR information, which includes:

(1) Changing locks, lock combinations, or keypad codes when personnel knowledgeable of locks, lock combinations, or keypad codes no longer need to:

(a) Know the information; or

(b) Access BAR information;

(2) Removal from access lists, including physical eradication of an individual's access privileges;

(3) Termination or deletion of an individual's access privileges to BAR information for which the individual currently has authorization and need-to-know access when the authorization and need-to-know access no longer exists; and

(4) Returning to the trusted partner any access devices, such as:

(a) Keys;

(b) Tokens;

(c) Badges; or

(d) Cards; and

H. Training for all personnel concerning the vulnerabilities of the BAR information and ways to ensure the protection of BAR information, which include:

(1) Awareness training including:

(a) Password maintenance;

(b) Security incident reporting; and

(c) Viruses and other forms of malicious software;

(2) Periodic security reminders of security concerns; and

(3) User education in:

(a) What to do if a virus is detected;

(b) Monitoring logon success or failure;

(c) How to report discrepancies; and

(d) Password management, including the:

(i) Rules to be followed in creating and changing passwords; and

(ii) Need to keep passwords confidential.

10.10.11.21

.21 BAR Information Security — Physical Safeguards.

A trusted partner shall establish physical safeguards to guard BAR information integrity, confidentiality, and availability, which include:

A. Physical protection of the personal computer system used for viewing BAR information and related buildings and equipment from:

(1) Fire;

(2) Natural and environmental hazards;

(3) Disasters; and

(4) Intrusion;

B. A secure work station location with physical safeguards to eliminate or minimize the possibility of unauthorized access to BAR information, including:

(1) Locating a personal computer used to access and view BAR information in a locked room;

(2) Restricting access to the locked room to authorized personnel by using:

(a) Electronic keypads;

(b) Electronic access badges; or

(c) Door locks;

(3) Placing the computer monitor in a way that screen contents are not viewable by an unauthorized person from within or outside the room;

(4) Locking file cabinets, desks, and desk drawers that contain BAR information:

(a) During nonworking hours; and

(b) When the BAR information custodian is not present in the immediate area; and

(5) Making BAR information nonviewable or unobtainable before admitting an unauthorized person into the workspace;

C. BAR information media control procedures that govern the receipt, removal, and disposal of BAR information CD-R discs into or out of the facility, which include:

(1) Access control so that only the BAR information custodian can receive the BAR information media;

(2) Accountability procedures that trace the receipt, removal, and disposal of BAR information media;

(3) BAR information storage; and

(4) Tracking the disposal process and the final disposition of:

(a) Electronic BAR information; and

(b) BAR information hardware on which electronic BAR information is stored;

D. Physical access controls that limit access of unauthorized personnel while ensuring that properly authorized access is allowed;

E. Emergency mode operation access controls that enable continuing protection to BAR information in the event of:

(1) Fire;

(2) Vandalism;

(3) Natural disaster; or

(4) BAR information computer information system failure;

F. A facility security plan to safeguard BAR information on the premises from unauthorized physical access, tampering, and theft;

G. Verifying access authorizations before granting physical access;

H. Maintaining documentation of repairs and modifications to the physical components of the facility including:

(1) Hardware;

(2) Walls;

(3) Doors; and

(4) Locks; and

I. Procedures governing the reception and hosting of visitors, including:

(1) Sign-in logs for visitors; and

(2) Providing escorts for visitors, if appropriate.

10.10.11.22

.22 BAR Information Security — Technical Security Measures.

A trusted partner shall establish a system of technical security measures to protect BAR information integrity, confidentiality, and availability, which include:

A. A BAR information security assessment to determine the sensitivity, vulnerabilities, and security of the trusted partner's programs and operations related to the BAR information the trusted partner:

(1) Receives;

(2) Views;

(3) Manipulates;

(4) Stores; or

(5) Transmits;

B. An information system certification based on a technical evaluation as part of and in support of the security process, which establishes the extent to which the trusted partner's computer system used for BAR information meets the security requirements of this chapter;

C. Making access to BAR information available only with a freestanding PC (personal computer) that has no:

(1) Connection to:

(a) The Internet;

(b) An intranet; or

(c) A network; and

(2) External devices connected such as a:

(a) Portable hard drive;

(b) Removable memory card; or

(c) Flash memory device;

D. Establishing and utilizing procedures and processes to guard against unauthorized access to BAR information by using:

(1) Access controls that include:

(a) Emergency role-based access of BAR information that documents the instructions for obtaining BAR information during a crisis;

(b) User-based access; and

(c) The use of encryption and decryption;

(2) An alarm that can sense an unauthorized access within the computer system and produce a signaled response such as a:

(a) System closure;

(b) Time-phased automatic shutdown and restart cycle; or

(c) Screen indicating a multiple password failure lockout;

(3) Audit controls that record and examine system activity;

(4) Audit trails of the use of and access to BAR information collected and used to facilitate a security audit; and

(5) Event reporting that shows a screen message indicating an unauthorized request for BAR information access.

E. Establishing procedures and processes for computer system authorization control for an individual to obtain access for the use and disclosure of BAR information, which include:

(1) Role-based access;

(2) User-based access;

(3) BAR information authentication that corroborates that BAR information has not been altered or destroyed in an unauthorized manner by using a:

(a) Message authentication code; or

(b) Digital signature;

(4) BAR information custodian authentication that includes:

(a) Automatic logoff that causes an electronic session to terminate after a predetermined time of inactivity; and

(b) A unique user identifier:

(i) Made up of a combination alpha and numeric characters; and

(ii) Maintained in security procedures for identifying and tracking individual user identity; and

(5) A logon mechanism using a:

(a) Password;

(b) Personal identification number (PIN);

(c) Token; or

(d) Any combination of §E(5)(a)—(c) of this regulation;

F. A security configuration management plan that includes:

(1) A written security plan documenting the rules, procedures, and instructions concerning all components related to BAR information security;

(2) Hardware and software installation and maintenance reviews;

(3) Security testing to ensure that the selected security features are:

(a) Implemented as designed; and

(b) Adequate for the operational environment; and

(4) Virus checking on a routine and regular basis;

G. Security incident procedures that describe how to:

(1) Report security incidents and breaches; and

(2) Respond to and take action as a result of the receipt of a security incident report; and

H. Sanction policies and procedures describing the disciplinary actions and notice of possible civil or criminal penalties an individual may be subject to for misuse or misappropriation of BAR information.

10.10.11.23

.23 Trusted Partner Agreement.

A. Requirement. The Department may not share BAR information with a person until the person becomes a trusted partner by entering into a trusted partner agreement, using the form developed by the Department.

B. The Department shall develop and use a trusted partner form that contains, as applicable, separate clauses that:

(1) Establish the length of time that the trusted partner agreement is in effect;

(2) Address that confidentiality will survive the termination, expiration, or cancellation of the trusted partner agreement and state that the trusted partner:

(a) May not use BAR information in a way that is detrimental to the Department;

(b) Shall keep BAR information confidential;

(c) Shall limit disclosure of BAR information only:

(i) To individuals with a legitimate need in performance of the individuals' duties; and

(ii) On a need-to-know basis as prescribed by this chapter; and

(d) Shall employ security policies that:

(i) Protect the confidentiality of BAR information; and

(ii) Prevent improper disclosures or access to BAR information;

(3) Require the trusted partner to notify the Department whenever the trusted partner discloses BAR information as allowed by this chapter;

(4) Warrant and represent that the trusted partner is in compliance with all applicable State and federal laws and regulations regarding BAR information;

(5) Require the trusted partner to execute a trusted partner agreement that upholds the standards and requirements in the trusted partner agreement that the trusted partner has with the Department;

(6) Require the trusted partner to notify the Department when there is:

(a) An improper or unauthorized:

(i) Disclosure of BAR information; or

(ii) Access to BAR information;

(b) A misuse of BAR information;

(c) A computer information system compromise that affects BAR information; or

(d) An authorized release of BAR information as set forth in this chapter;

(7) Address corrective action by stating:

(a) The steps necessary to prevent any further unauthorized disclosure and misuse of BAR information;

(b) That the trusted partner shall maintain an incident log of all unauthorized disclosures and misuse of BAR information; and

(c) That the trusted partner shall send a copy of incident log entries to the BAR Program;

(8) Require the trusted partner to:

(a) Return the BAR information that was provided to the trusted partner; and

(b) Exercise due diligence to destroy all material based on BAR information in a manner that renders nonidentifiable all documents, memoranda, notes, or other writings created or prepared by or for the trusted partner or BAR information custodian;

(9) Require the trusted partner to make available on demand to the Department all policies and procedures relevant to safeguarding BAR information;

(10) Address the authority of the individuals signing the trusted partner agreement that state that:

(a) The individuals signing the trusted partner agreement have the right and authority to execute the agreement on behalf of their respective entity; and

(b) No further approvals are necessary to make the trusted partner agreement binding;

(11) State that the trusted partner agreement is the entire agreement between the Department and the trusted partner;

(12) State that the trusted partner agreement may not be amended, except as agreed to by the Department in writing;

(13) State that no provision or clause in the trusted partner agreement may be waived unless approved in writing by the Department;

(14) Identify the individual designated by the trusted partner and authorized by the Department to receive, maintain, and if provided by this chapter, release BAR information;

(15) Attest that the BAR information custodian has the trusted partner's agency clearance to receive BAR information;

(16) Address a trusted partner's security policy that states the:

(a) Value of BAR information;

(b) Protection responsibilities; and

(c) Organizational commitment for a system to protect the integrity, confidentiality, and availability of BAR information; and

(17) State that if a provision, section, subsection, sentence, clause, or phrase of the trusted partner agreement is held invalid, the remaining portions of the trusted partner agreement remain valid.

10.10.11.24

.24 Penalties.

A. Fine. A person who violates a provision of Health-General Article, Title 17, Subtitle 6, Annotated Code of Maryland, or this chapter is guilty of a misdemeanor and on conviction is subject to a fine not exceeding $100 for the first offense and not exceeding $500 for each subsequent conviction for a violation of the same provision.

B. Subsequent Offense. Each day a violation is continued after the first conviction is a subsequent offense.

10.10.11.9999

Administrative History

Effective date: November 25, 2002 (29:23 Md. R. 1811)

Chapter revised effective July 31, 2006 (33:15 Md. R. 1280)

Chapter revised effective January 23, 2012 (39:1 Md. R. 17)