CITY OF PHILADELPHIA

DEPARTMENT OF PUBLIC HEALTH

CONFIDENTIALITY POLICY

(Version 1.0 – 7/10/14)

TABLE OF CONTENTS

I. DEFINITIONS

The following words and terms are defined for purposes of this Confidentiality Policy only:

Authorization Form: The form by which a Data Subject permits the Department to disclose the Data Subject's Confidential Information to another person or organization.

Board of Health: The Board of Health of the City of Philadelphia.

City: The City of Philadelphia.

Commonwealth: The Commonwealth of Pennsylvania.

Confidential Information: Any information, whether oral, paper-based, electronic, visual, pictorial, physical, or in any other form, including, but not limited to, medical and demographic information and information relating to services, the provision of Health Care, funding for Health Care, or other benefits provided by the Department, that: (a) reveals the identity of any individual or is readily identified with any individual; or (b) provides a reasonable basis to believe that the information could be used, either alone or in combination with other information, to identify any individual. For purposes of this Confidentiality Policy, Confidential Information shall not include any information appropriately collected, used, or disclosed by the Department in connection with the everyday operations of the Department's Human Resources Office.

Contractor: Any individual or entity (private non-profit, private for-profit, or public) with which the Department has a fully-executed contract to provide services or goods.

Data Subject: Any individual who is identifiable pursuant to the definition of Confidential Information.

Department: Philadelphia Department of Public Health.

Employee: Any officer or employee (including City and contracted employees) of the Department, and any intern, fellow, student, or volunteer who performs work for or on behalf of the Department.

Health Care: Care, services, or supplies related to the health of an individual including, but not limited to, the following: preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure related to the physical, mental, behavioral, or functional condition of an individual; or sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Operations: Administrative, financial, legal, and quality improvement activities that are necessary for the operation and support of core functions of treatment and payment,

including, but not limited to, quality assessment; contacting health care providers and patients with information about treatment; reviewing competence or qualifications of health care professionals; accreditation, certification, licensing, and credentialing activities; conducting or arranging medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; business planning and development; and business management and general administrative activities.

HIPAA Covered Component: A division of the Department that has been designated by the City as a unit that must comply with the Privacy and Security Rules promulgated pursuant to the Health Insurance Portability and Accountability Act.

Program Evaluation: A systematic evaluation of a Department program or service against specific benchmarks or other criteria designed to increase efficacy.

Public Health Intervention: A program or service that seeks to achieve a Public Health Purpose.

Public Health Investigation: A detailed inquiry or systematic examination for a Public Health Purpose.

Public Health Purpose: A purpose relating to a population-based activity or individual effort primarily aimed at the prevention of injury, disease, or premature mortality, or the promotion of health in the community, including but not limited to: (a) assessing the health needs and status of the community through public health surveillance and epidemiology; (b) developing public health policy; and (c) responding to public health needs and emergencies.

Quality Improvement: The assessment of Department products, services, programs, treatments, provisions of care, funding, or other benefits, for the purpose of improvement. These activities are often carried out repeatedly over time.

Research: A systematic investigation, including development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Activities which meet this definition constitute Research for purposes of this Confidentiality Policy, whether or not they are conducted or supported under a program which is considered research.

Surveillance: A type of observational study that involves continuous monitoring or close supervision of disease occurrence, indications of disease occurrence, or risk factors associated with disease occurrence, within a population.

Unauthorized Disclosure: The intentional or inadvertent disclosure of Confidential Information.

II. EXECUTIVE SUMMARY

A. Purpose

To further its mission, the Philadelphia Department of Public Health (the "Department") collects, uses, and discloses Confidential Information, as appropriate, for public health surveillance, program development and implementation, program evaluation and quality improvement, and for other Public Health Purposes. The Department also collects information from individuals seeking certain services or benefits. It is critical that Department Employees recognize the importance of protecting, to the greatest extent possible, personal privacy and safeguarding the confidentiality of information obtained by the Department. This Confidentiality Policy sets out the Department's requirements and procedures, and the responsibilities of Employees, directors of divisions and offices, and designated Confidentiality Liaisons.

B. Application

This Confidentiality Policy applies to all officers and employees (including City and contracted employees) of the Department, and all interns, fellows, students, and volunteers who perform work for or on behalf of the Department. The Department shall enter into confidentiality agreements, as needed, with non-Employee contracted individuals and organizations.

C. Relation to Other Laws and Policies

Employees may be subject to additional standards and requirements adopted and maintained by their division or office. In addition, an Employee working for or on behalf of a HIPAA Covered Component is subject to the HIPAA policies and procedures applicable to that division or office, which set forth additional standards and requirements relating to confidentiality of individually identifiable health information. An updated list of HIPAA Covered Components shall be maintained by the Department.

D. Key Components of the Policy

(1) Limited Collection, Use, and Disclosure of Confidential Information

Employees may collect, use, or disclose Confidential Information only when:

(i) The collection, use, or disclosure of such information is consistent with applicable laws and regulations; and

(ii) The collection, use, or disclosure of such Confidential Information is:

(a) Authorized by the Data Subject pursuant to Section III(B); or

(b) Reasonably necessary for a Public Health Purpose (e.g., Program Evaluation, Quality Improvement, payment verification, Public Health Investigation, Surveillance, Public Health Intervention, Health Care, or Health Care Operations); or

(c) Reasonably necessary to provide or offer City services, funding, or other benefits to the Data Subject; or

(d) Mandated pursuant to applicable laws or regulations, and the collection, use, or disclosure is consistent with and reasonably necessary for carrying out the intent of such laws or regulations.

Employees shall use or disclose no more Confidential Information than is reasonably necessary to accomplish their work.

An Employee's access to Confidential Information shall be limited, as feasible, to what is necessary for the Employee's work by the Employee's supervisors.

(2) Security and Storage of Confidential Information

Employees who have access to Confidential Information shall ensure that such information is stored, maintained, and disclosed in a secure manner that prevents unauthorized individuals from gaining access to such information either intentionally or inadvertently.

Employees shall be provided with adequate means with which to comply with the data security requirements of this Confidentiality Policy.

(3) Data Destruction

Confidential Information in any destructible form, including electronic media and data, must be destroyed consistent with this Confidentiality Policy in order to ensure that unauthorized individuals cannot obtain access to such information.

(4) Policies and Procedures Regarding Disclosure

When applicable, the Data Subject must provide authorization for disclosure of his or her Confidential Information as outlined in this Confidentiality Policy. When data are disclosed for a Public Health Purpose or to provide a service or benefit, Employees should follow the procedures described in this Confidentiality Policy, including the use of confidentiality agreements when appropriate.

(5) Policies and Procedures Regarding Confidentiality Policy Compliance

All Employees are required to comply with this Confidentiality Policy. Employees shall immediately report any violations of this Confidentiality Policy to their supervisor or their Confidentiality Liaison. The Confidentiality Officer will be responsible for investigations and, in conjunction with the Department's Human Resources Office and the Law Department, will take appropriate corrective actions in the event this Confidentiality Policy is violated. Employees are protected from retaliation for reporting another Employee's violation of the Confidentiality Policy.

(6) Administration and Training

The Health Commissioner will appoint a Department Confidentiality Officer to oversee implementation, evaluation, and, as needed, revision of the Confidentiality Policy. In addition, each division or office within the Department shall designate, with approval by the Confidentiality Officer, an Employee as the Confidentiality Liaison for that division or office, and this person shall aid in the implementation and evaluation of this Confidentiality Policy. Every Employee will receive training on the Confidentiality Policy and provide written acknowledgment of the training.

[REMAINDER OF THIS PAGE IS BLANK]

III. TREATMENT OF CONFIDENTIAL INFORMATION

Purpose: The intent of this section is to instruct on when the collection, use, or disclosure of Confidential Information is permissible; how to procure from Data Subjects authorization to collect, use, and disclose Confidential Information that pertains to them; data security requirements concerning the use, storage, and disclosure of Confidential Information; and the protocol for the destruction of Confidential Information.

A. Collection, Use, and Disclosure of Confidential Information

Purpose: The intent of this section is to instruct on when and under what circumstances Employees may collect, use, or disclose Confidential Information from Data Subjects. This section also instructs on documentation requirements for authorized disclosures.

(1) Employees may collect, use, or disclose Confidential Information only when:

(i) The collection, use, or disclosure of such information is consistent with applicable laws and regulations; and

(ii) The collection, use, or disclosure of such Confidential Information is:

(a) Authorized by the Data Subject pursuant to Section III(B); or

(b) Reasonably necessary for a Public Health Purpose (e.g., Program Evaluation, Quality Improvement, payment verification, Public Health Investigation, Surveillance, Public Health Intervention, Health Care, or Health Care Operations); or

(c) Reasonably necessary to provide or offer City services, funding, or other benefits to the Data Subject; or

(d) Mandated pursuant to applicable laws or regulations, and the collection, use, or disclosure is consistent with and reasonably necessary for carrying out the intent of such laws or regulations.

(2) Confidential Information may not be collected, used, or disclosed:

(i) In any way that conflicts with restrictions made by the Data Subject on an Authorization Form, if the permissibility of the disclosure of Confidential Information is predicated on an Authorization Form. (See Section III(B).)

(ii) By Employees for any reason other than the performance of their work for or on behalf of the Department.

(iii) By Employees any time after separation from the Department. This Confidentiality Policy continues to apply to Employees after they leave the Department with respect to Confidential Information to which Employees had access while working for or on behalf of the Department.

(3) Access to Confidential Information

(i) An Employee's access to Confidential Information shall be limited by the Employee's supervisors, as feasible, to what is necessary for the Employee's work.

(ii) An Employee shall not share Confidential Information with another Employee except in furtherance of work for the Department.

(iii) An Employee who shares Confidential Information with another Employee in compliance with Section III(A)(3)(ii) is not "disclosing" Confidential Information for purposes of this Confidentiality Policy. Such sharing of Confidential Information between Employees is not subject to the additional requirements of Sections III(A)(4) and (5); however, all other applicable provisions remain in effect.

(4) Required approvals for disclosure of Confidential Information

(i) Public Health Purpose: An Employee may disclose Confidential Information for a Public Health Purpose (e.g., public health investigation, surveillance, public health intervention) with the approval of the Confidentiality Officer, the Confidentiality Liaison of the division or office disclosing the Confidential Information, and the director of the division or office disclosing the Confidential Information. If the Department contracts with the recipient of the disclosure, that contract must include a confidentiality agreement in accordance with Section III(A)(5).

(ii) Provision or offering of City services, funding, or benefits: Disclosure of Confidential Information in order to provide or offer a City service, funding, or benefit is permissible with the approval of the Confidentiality Officer, the Confidentiality Liaison of the division or office disclosing the Confidential Information, and the director of the division or office disclosing the Confidential Information. If the Department contracts with the recipient of the disclosure, that contract must include a confidentiality agreement in accordance with Section III(A)(5).

(iii) City Law Department: To facilitate the Law Department's provision of effective legal counsel to the Department, Employees may disclose

Confidential Information to the Law Department with the approval of the Confidentiality Officer, the Confidentiality Liaison of the division or office disclosing the Confidential Information, and the director of the division or office disclosing the Confidential Information.

(iv) Court order or other legal process: Disclosure of Confidential Information specified by judicial order or other legal process is permissible with the approval of the Law Department, the Confidentiality Officer, the Confidentiality Liaison of the division or office disclosing the Confidential Information, and the director of the division or office disclosing the Confidential Information.

(v) State or federal government as mandated by law: Disclosure of Confidential Information to state or federal government agencies as required by law is permissible with the approval of the Confidentiality Officer, the Confidentiality Liaison of the division or office disclosing the Confidential Information, and the director of the division or office disclosing the Confidential Information.

(vi) City and Department Investigations: Confidential Information may be disclosed in order to facilitate an investigation by the City or Department with the approval of the Health Commissioner.

(5) Confidentiality agreements are required when the Department discloses Confidential Information for a Public Health Purpose or for the provision or offering of City services, funding, or benefits to a person or entity with whom the Department contracts.

(i) The confidentiality agreement must describe the type of Confidential Information being disclosed, the method of disclosure, the period of time for which the confidentiality agreement shall remain in effect, the reason for the disclosure, the persons within the Contractor who shall have access to the Confidential Information, any prohibitions on the use or disclosure of the Confidential Information for any other purpose, how the Confidential Information will be secured, and the Contractor's responsibility to retain, return, or dispose of the Confidential Information when the confidentiality agreement terminates.

(ii) The confidentiality agreement must be approved by the Law Department, the Confidentiality Officer, the Confidentiality Liaison of the division or office disclosing the Confidential Information, and the director of the division or office disclosing the Confidential Information.

(6) Additional requirements for Research

(i) Disclosure of Confidential Information to a person for purposes of Research is permissible following approval by the Confidentiality Officer and Liaison and the division director; review and approval by the Department's Institutional Review Board; and execution of a data license agreement.

(ii) The data license agreement must be approved by the Law Department, the Health Commissioner, the Confidentiality Officer, the Confidentiality Liaison of the division or office disclosing the Confidential Information, and the director of the division or office disclosing the Confidential Information.

(iii) The process for sharing City generated or maintained data from the Office of the Deputy Mayor for Health and Opportunity (or its equivalent) for the purpose of Research is available here:

http://www.phila.gov/health/pdfs/External%20Research%20Requests.pdf

(iv) The Institutional Review Board process is available here:

http://www.phila.gov/health/Commissioner/IRB.html

(7) Disclosures not identified in Sections III(A)(4), (5), or (6) **require approval by the Confidentiality Officer and Liaison, a Data Subject Authorization Form**, and any other approvals the Confidentiality Officer deems necessary.

(8) Collection of Approvals

The Confidentiality Officer shall coordinate the collection of approvals in accordance with Section V(A)(1)(iv).

(9) HIPAA Covered Components

For Employees in HIPAA Covered Components, where this Section III(A) conflicts with the policies and procedures of the HIPAA Covered Component concerning disclosure of Personal Health Information, Section III(A) does not apply.

(10) Other Laws and Policies

This Confidentiality Policy does not comprehensively delineate all requirements for disclosures related to Confidential Information. It is incumbent upon the Department and its Employees to comply with all applicable laws and policies.

B. Data Subject Authorization for Disclosure of Confidential Information

Purpose: The intent of this section is to instruct on what constitutes a valid authorization for the disclosure of Confidential Information. This section specifies the required content of Authorization Forms and the record retention schedule for these forms.

(1) Disclosure of Confidential Information shall not be deemed authorized by any Data Subject unless authorization is given pursuant to the standards and requirements set forth in this section.

(i) The Department may disclose Confidential Information if authorized and directed by the Data Subject. The Data Subject or his or her authorized representative must complete an Authorization Form directing the Department to disclose the Data Subject's Confidential Information.

(ii) Authorization Forms must contain all of the following information:

(a) The specific name or general designation of the program or person permitted to make the disclosure;

(b) The name or title of the individual, or the name of the organization to which the disclosure is to be made;

(c) The name of the subject;

(d) The date of birth of the subject;

(e) The purpose of the disclosure;

(f) How much and what kind of information is to be disclosed;

(g) The signature of the subject;

(h) The date on which the consent is signed;

(i) A written statement that the consent is subject to revocation at any time except to the extent that the person who is to make the disclosure has already acted in reliance on it; and

(j) The date (not to exceed one year), event, or condition upon which the consent will expire, if not earlier revoked.

(iii) Authorization Forms must be completed using ink (e.g., pen, printer, typewriter). No corrections shall be made on the Authorization Form (e.g., cross-outs,

correction fluid/tape), unless accompanied by a full signature next to each correction.

(iv) All Authorization Forms shall be retained by the Department on a network drive for a minimum of six years.

(v) Procedure for disclosure of Confidential Information pursuant to an Authorization Form:

(a) Verify that the Authorization Form conforms to the requirements set forth in Section IV(B)(1)(ii).

(b) Verify that the Authorization Form has not expired.

(c) Disclose only information identified in the Authorization Form

(d) Disclose only to the party identified in the Authorization Form.

(e) Include the following written statement pursuant to 35 P.S. § 7607 if applicable:

This information has been disclosed to you from records protected by Pennsylvania law. Pennsylvania law prohibits you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or is authorized by the Confidentiality of HIV-Related Information Act. A general authorization for the release of medical or other information is not sufficient for this purpose.

(f) Include the following written statement pursuant to 42 C.F.R. § 2.32 if applicable:

This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is ***NOT*** *sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.*

(g) Comply with all other applicable laws and policies. Sections VI and VII contain laws and policies that may be applicable.

C. Data Security for the Use, Storage, and Disclosure of Confidential Information

Purpose: The intent of this section is to instruct on the security and storage requirements for Confidential Information, including during the process of disclosure, in order to ensure that unauthorized individuals cannot obtain access to Confidential Information. The provisions of this section also help to ensure that Employees do not inadvertently view or handle Confidential Information that they are not authorized to access.

(1) Workstation and Device Security

(i) Employees who handle Confidential Information must abide by the following rules to preserve workstation and device security:

(a) Passwords may not be shared.

(b) No Employee may allow anyone to use a Department desktop computer, laptop, tablet, phone, or other electronic device while it is operating under the Employee's username and password, unless the use is necessary for the Employee's work and the Employee supervises the use. Similarly, no Employee may use any Department desktop computer, laptop, tablet, phone, or other electronic device while it operates under another Employee's username and password, unless the Employee to whom the username is assigned permits and supervises the use.

(c) Documents containing Confidential Information must be covered, turned face-down, or put away when the workstation is unattended for any period of time. When the workstation will be unattended for more than an hour, and at the end of each day, documents containing Confidential Information must be stored and maintained pursuant to Section III(C)(2)(ii).

(d) Desktop computers, laptops, tablets, phones, or other electronic devices, including but not limited to removable media and portable devices, must be electronically locked or shut down at any time the device is unattended. When unattended for more than an hour, portable electronic devices that may easily be stolen (including but not limited to laptops, tablets, phones, and removable media) shall be stored and maintained pursuant to Section III(C)(2)(iii).

(2) Storage of Confidential Information

(i) Employees who handle Confidential Information shall ensure that such information is stored and maintained in a secure manner that prevents unauthorized individuals from gaining access to such information.

(ii) Storage of paper-based Confidential Information

(a) Employees shall not leave Confidential Information unattended for more than an hour or at the end of the day without employing adequate safeguards against unauthorized access. Safeguards include but are not limited to the following:

(1) Employees shall store Confidential Information in a locked desk or cabinet. A single key should not open more than one lock.

(2) If Employees are unable to store Confidential Information in a locked desk or cabinet, Employees shall secure the worksite by locking all access doors.

(b) Documents in long-term storage shall, at a minimum, be contained in a room that is routinely kept locked, with access limited to Employees authorized to access the Confidential Information therein.

(c) Printers, copiers and fax machines

(1) Employees who handle Confidential Information shall ensure that such information, if produced or reproduced using a printer, copier, fax machine, or similar device shall be retrieved immediately.

(2) Printing or other reproduction of Confidential Information shall be minimized.

(iii) Storage of electronic Confidential Information:

(a) Employees who handle electronic Confidential Information shall ensure that such information shall be stored and maintained pursuant to the following requirements:

(1) Files containing Confidential Information stored on Department networks, desktop computers, laptops, tablets, phones, or other electronic devices, including but not limited to removable media and portable devices, must be password protected and, as feasible, encrypted. Individual files do not need to be password protected so

long as they reside in folders, subfolders, or drives that are password protected.

(2) Department networks, desktop computers, laptops, tablets, phones, or other electronic devices containing Confidential Information, including but not limited to removable media and portable devices, must be password protected and, as feasible, encrypted.

(3) Electronic devices containing Confidential Information shall be electronically locked or shut down while not in use or unattended by an Employee using such device. While not in use or unattended by an Employee, electronic devices that may be easily stolen or improperly removed must either be placed in a locked desk or cabinet, or secured in a locked room, with access limited to authorized individuals only.

(4) Confidential Information shall only be stored on Department owned and maintained networks, desktop computers, laptops, tablets, phones, or other electronic devices, including but not limited to removable media and portable devices. Notwithstanding the foregoing, remote databases may be utilized to perform the work of the Department when required by state or federal agencies.

(3) Removal of Confidential Information from the worksite

(i) Employees shall not remove Confidential Information from the worksite unless reasonably necessary for a field visit, meeting, or other work-related purpose. Removal of Confidential Information requires permission from a direct supervisor and the Confidentiality Liaison within the division or office.

(ii) Paper-based Confidential Information: If an Employee removes paper-based Confidential Information from the worksite, he or she must:

(a) Ensure that the Confidential Information is not left unattended if it can be accessed or taken by unauthorized individuals.

(b) Use a locking travel file if available.

(iii) Portable electronic devices: If an Employee removes electronic devices containing Confidential Information from the worksite, he or she must:

(a) Ensure that laptops, tablets, phones, or other electronic devices, including but not limited to removable media and portable devices, are

not left unattended if they can be accessed or taken by unauthorized individuals.

(b) Ensure that when laptops, tablets, phones, or other electronic devices, including but not limited to removable media and portable devices, are left unattended in an automobile, the automobile is locked and any device is kept out of sight to minimize the risk of theft.

(c) Not allow any person not authorized to handle the Confidential Information to use any laptop, tablet, phone, or other electronic device, including but not limited to removable media and portable devices, containing such information.

(iv) If Confidential Information is lost or stolen, the Employee responsible for the Confidential Information shall within one business day notify his or her supervisor and Confidentiality Liaison.

(4) Disclosure of Confidential Information

(i) Special requirements governing disclosure of paper-based Confidential Information via hand delivery, fax, inter-office mail, regular mail, or delivery or courier service

(a) Hand delivery. Employees disclosing Confidential Information pursuant to this Policy via hand delivery to an authorized recipient must ensure that the Confidential Information is not visible during transport.

(b) Fax. An Employee sending Confidential Information via fax must:

(1) Verify that the correct Confidential Information is being faxed to the correct person and verify the fax number of the intended recipient.

(2) Inform the recipient, verbally or in writing, that the Employee is sending Confidential Information through fax and, before sending the fax, request verification that the recipient is there to receive the fax or that the fax machine is located in a secure area.

(3) Include a cover letter or memorandum addressed to the intended recipient and marked "Confidential." The cover letter or memorandum must contain instructions directing an unauthorized recipient of a misdirected fax to contact the sender. In the event of a misdirected fax, the unauthorized recipient should be directed to shred the fax immediately and notify the sender.

(4) Remove the faxed document containing Confidential Information, including the fax activity confirmation sheet, from the fax machine after the fax is transmitted. Retain the fax activity confirmation sheet with the original document for a minimum of three months.

(c) Inter-departmental mail. Employees sending Confidential Information via inter-departmental mail must:

(1) Verify that the correct Confidential Information is being mailed to the correct person and verify the office location of the intended recipient.

(2) Send the Confidential Information in a security envelope marked "Confidential" and seal the envelope.

(3) If leaving Confidential Information in an outgoing mailbox or container, ensure that the mailbox or container is approved for such use by the division or office.

(d) U.S. mail. Employees sending Confidential Information via U.S. mail must:

(1) Verify that the correct Confidential Information is being mailed to the correct person and verify the address of the intended recipient.

(2) Send the Confidential Information in a security envelope marked "Confidential" and seal the envelope.

(3) Whenever feasible, send the Confidential Information by registered or certified mail, or another method that provides delivery tracking.

(4) If leaving Confidential Information in an outgoing mailbox or container, ensure that the mailbox or container is approved for such use by the division or office.

(e) Delivery or courier service. Employees sending Confidential Information via delivery or courier service must:

(1) Verify that the correct Confidential Information is being sent to the correct person and verify the address of the intended recipient.

(2) Send the Confidential Information in a security envelope marked "Confidential" and seal the envelope.

(3) Retain a tracking number or other means of tracking the delivery.

(4) If leaving Confidential Information in an outgoing mailbox or container, ensure that the mailbox or container is approved for such use by the division or office.

(ii) Special rule governing verbal disclosure of Confidential Information (via telephonic communication)

No Confidential Information should be given to someone who calls the Department and requests information over the phone unless it is established that the caller is an authorized recipient of such information and can prove his or her identity. For example, the caller's identity and phone number should be verified by phoning the caller back at a number known to be associated with the authorized recipient.

(iii) Special rules governing the disclosure of electronic Confidential Information

(a) Only the following listed methods of disclosing electronic Confidential Information shall be permitted:

(1) Password protected and, as feasible, encrypted Department networks

(2) Encrypted Department FTP servers

(3) The following types of removable media:

(i) Password protected and, as feasible, encrypted USB memory stick or flash drive

(ii) Password protected and, as feasible, encrypted CD or DVD

(b) Special rules governing use of e-mail

(1) Disclosure of Confidential Information via e-mail is prohibited without written permission from the Confidentiality Officer.

(2) All e-mail shall be accompanied by a confidentiality disclaimer approved by the Confidentiality Officer.

(5) Additional Requirements

(i) Employees are accountable for handling data in a manner consistent with any and all governing data use agreements and commonly accepted practices for guarding against potential subject identification.

(ii) Employees are responsible for compliance with any additional data security requirements imposed by their respective divisions or offices.

(6) Employees shall be provided with adequate means with which to comply with the data security requirements of this Confidentiality Policy.

D. Destruction of Confidential Information

Purpose: The intent of this section is to instruct on the destruction of Confidential Information in order to ensure that unauthorized individuals cannot obtain access to such information.

(1) Paper-based Confidential Information

(i) Employees disposing of paper-based Confidential Information must ensure that such information is destroyed using shredders (preferably crosscutting shredders) in place within the division or office.

(2) Electronic Confidential Information

(i) In collaboration with the Department's Informational Technology Division, Employees disposing of electronic Confidential Information on desktop computers, laptops, tablets, phones, or other electronic devices, including but not limited to removable media and portable devices, must delete and destroy the Confidential Information so that it cannot be recovered from the storage media. Employees must use an approved file destruction process to ensure proper destruction of Confidential Information.

(ii) Desktop computers, laptops, tablets, phones, and other electronic devices used at any time to store Confidential Information, including but not limited to removable media and portable devices, must be properly destroyed, or have all data storage components destroyed, upon completion of their use by the Department. Employees shall coordinate with the Informational Technology Division of the Department to ensure proper destruction.

[REMAINDER OF THIS PAGE IS BLANK]

IV. UNAUTHORIZED DISCLOSURE AND NON-COMPLIANCE

Purpose: The intent of this section is to instruct on the appropriate procedures when there is an Unauthorized Disclosure and when an Employee violates this Confidentiality Policy.

A. Compliance Requirement

(1) All Employees are required to comply with this Confidentiality Policy.

(2) Employees who fail to comply may be denied further access to Confidential Information and may be subject to disciplinary action, up to and including termination.

B. Reporting Requirement

(1) Any Employee who becomes aware of an Unauthorized Disclosure or a violation of this Confidentiality Policy must report the incident within one business day to:

Health-Confidentiality@phila.gov

The initial report need not include details.

(2) Any Employee who fails to report an Unauthorized Disclosure or a violation of this Confidentiality Policy in a timely manner may be subject to appropriate disciplinary action.

C. Protection for Reporting Employees

(1) An Employee who is first to report his or her own violation of this Confidentiality Policy shall receive favorable consideration for so reporting when appropriate disciplinary action, if any, is determined.

(2) An Employee who reports an Unauthorized Disclosure or another Employee's actual or suspected violation of this Confidentiality Policy in good faith shall be protected from retaliation by any other Employee for so reporting. Appropriate disciplinary action is not retaliation.

D. Investigation

(1) The Confidentiality Officer is responsible for managing the investigation of all reported Unauthorized Disclosures and all reported violations of this Confidentiality Policy. The Confidentiality Officer shall identify and implement appropriate corrective measures and disciplinary actions, if any, in conjunction with the Department's Human Resources Office, appropriate IT personnel, the director of the

division or office in which the Unauthorized Disclosure or violation occurred, and, as needed, the Law Department.

(2) If the suspected Unauthorized Disclosure or violation relates to a HIPAA Covered Component, the HIPAA Covered Component's HIPAA Privacy and Security Officer shall be notified by the Confidentiality Officer or Liaison and shall be involved in the investigation. Compliance with the HIPAA Covered Component's policies and procedures is required.

E. Notice to Affected Data Subjects

(1) The decision to notify affected Data Subjects shall be made on a case-by-case basis by the Confidentiality Officer, with approval by the Health Commissioner and in consultation with the Law Department, in consideration of the following factors:

(i) Any state or federal laws requiring notification, including but not limited to notifications required by HIPAA Breach Notification Rule and the Pennsylvania Breach of Personal Information Notification Act;

(ii) Risk of identity theft;

(iii) Risk of further damage if notification increases awareness of an Unauthorized Disclosure of Confidential Information;

(iv) Risk of physical harm of any individual;

(v) Risk of humiliation or damage to the reputation of the Data Subject; and

(vi) Risk of loss of business or employment opportunities for an individual.

[REMAINDER OF THIS PAGE IS BLANK]

V. ADMINISTRATION AND TRAINING

Purpose: The intent of this section is to instruct on the duties and responsibilities of the Confidentiality Officer, Confidentiality Liaisons, supervisors, and heads of divisions and offices in ensuring compliance with the terms, requirements, and spirit of this Confidentiality Policy.

A. Confidentiality Officer

(1) The Department shall have at all times one Confidentiality Officer. The Health Commissioner shall designate one City Employee to serve as the Department-wide Confidentiality Officer. The Confidentiality Officer's responsibilities include but are not limited to the following:

(i) Implement and administer this Confidentiality Policy on a Department-wide level.

(ii) Coordinate with all Confidentiality Liaisons, supervisors, and heads of divisions and offices to ensure consistent implementation and administration of this Confidentiality Policy.

(iii) Develop and update supporting documents for the Confidentiality Policy as needed (e.g., confidentiality agreement template).

(iv) Develop and implement a system for coordinating the collection of disclosure approvals required pursuant to Section III(A). The system should identify for any disclosed Confidential Information its type and to whom it is disclosed. Disclosing divisions and offices shall update periodically their disclosure recipients and the categories of Confidential Information disclosed.

(v) Coordinate with Confidentiality Liaisons, supervisors, heads of divisions and offices, and the Human Resources Office to develop and implement training for all Employees.

(vi) Coordinate with Confidentiality Liaisons and division directors to ensure that appropriate, functioning equipment and other means exist to facilitate Employee compliance with this Confidentiality Policy.

(vii) Inform the Health Commissioner and relevant division directors of any Unauthorized Disclosure of Confidential Information or any facilities, equipment, or training necessary to implement this Confidentiality Policy.

(viii) On an annual basis, coordinate with Confidentiality Liaisons and, if applicable, propose changes to this Confidentiality Policy to the Health Commissioner.

(ix) In accordance with Section IV(D), investigate all reported Unauthorized Disclosures and all reported violations of this Confidentiality Policy and identify and implement corrective measures and disciplinary action.

B. Confidentiality Liaisons

(1) Each director of a division or office shall designate a City Employee to serve as the Confidentiality Liaison for that division or office. The Confidentiality Liaison's responsibilities include but are not limited to the following for his or her division or office:

(i) Implement and administer this Confidentiality Policy in consultation with the division or office director.

(ii) Ensure that confidentiality training is properly administered to Employees and documented.

(iii) Work with the Confidentiality Officer to ensure adequate facilities and equipment are in place and properly maintained in the division or office so that Employees are able to abide by and fulfill the intent of this Confidentiality Policy.

(iv) Advise the Confidentiality Officer and relevant division director of any Unauthorized Disclosures and violations of this Confidentiality Policy.

(v) Advise the Confidentiality Officer on suggested changes to this Confidentiality Policy, as applicable.

(vi) Maintain procedures relating to requests for disclosure of Confidential Information.

(vii) Coordinate with staff and outside individuals and entities requesting Confidential Information to facilitate appropriate disclosure.

(viii) Manage and facilitate requests for Institutional Review Board approval.

(ix) Track each Employee's access to Confidential Information and permissions granted to each Employee for sharing Confidential Information, as allowable, by maintaining a current list or database with the following information:

(a) Job title or function;

(b) Types of Confidential Information that an Employee with the job title or function may access; and

(c) Role of an Employee with the job title or function in collecting, using, and/or disclosing that type of Confidential Information;

C. Training

(1) All Employees must receive training on this Confidentiality Policy, and any other related policy applicable to such Employee. Temporary Employees expected to be employed for fewer than 30 days may receive an abbreviated training deemed adequate by the Confidentiality Officer, but they are subject to the terms of this Confidentiality Policy and are required to acknowledge their understanding of it.

(2) If any material change is made to this Confidentiality Policy, Employees shall be informed of the change and required to acknowledge their understanding of the change. The Confidentiality Officer shall coordinate re-training for all Employees if the Health Commissioner determines that a material change warrants such re-training.

D. Acknowledgment

(1) Upon hire, all Employees, other than contracted Employees, shall receive from the Human Resources Office a copy of this Confidentiality Policy. The Employee shall acknowledge receipt and shall review the Confidentiality Policy and attend a training session.

(2) Upon hire, all contracted Employees shall receive from the hiring division or office a copy of this Confidentiality Policy. The contracted Employee shall acknowledge receipt and shall review the Confidentiality Policy and attend a training session.

(3) All Employees shall receive training on the Confidentiality Policy. The Employee who conducts the training shall procure from each attendee an acknowledgment of training, which shall include agreement to comply with the Confidentiality Policy.

(4) All acknowledgments for Employees other than contracted Employees shall be kept with the Employee's Human Resources file, while acknowledgments for contracted Employees shall be kept in the hiring division or office's files.

[REMAINDER OF THIS PAGE IS BLANK]

VI. ADDITIONAL STANDARDS AND REQUIREMENTS

Purpose: The intent of this section is to instruct on additional standards and requirements not explicitly outlined in this Confidentiality Policy.

A. Divisions and Offices

Employees are subject to additional standards and requirements set forth by their divisions or offices.

B. Policies Applicable to Certain Employees

(1) **HIPAA policies and procedures**. Applicable to HIPAA Covered Components in the Department and any individual in the Department who provides support services to a HIPAA Covered Component that involves access to individually identifiable health information created or maintained by the HIPAA Covered Component.

(2) **Institutional Review Board policy**. Applicable to any Research involving human subjects and supported by the Department of Public Health, the Office of Behavioral Health and Intellectual disability Services, the Department of Human Services, Office of Supportive Housing, or Philadelphia Prison Health Services. (http://www.phila.gov/health/Commissioner/IRB.html)

(3) **External Research requests for City generated or maintained data – Office of the Deputy Mayor for Health and Opportunity (or its equivalent)**. Applicable to data generated or maintained by the Department of Public Health, the Office of Behavioral Health and Intellectual disAbility, the Department of Human Services, and the Office of Supportive Housing. (http://www.phila.gov/health/pdfs/External%20Research%20Requests.pdf)

(4) **Policy relating to a Right-to-Know request** (see 65 P.S. § 67.101 *et seq.*). Applicable to any Employee who receives a Right-to-Know request seeking Department records. (http://www.phila.gov/privacy/pdfs/finalcityopenrecords.pdf)

(5) **Policy for Human Resources Employees**. Applicable to Employees in the Human Resources Office.

[REMAINDER OF THIS PAGE IS BLANK]

VII. LIST OF APPLICABLE STATE AND FEDERAL LAWS

Confidentiality of HIV-Related Information Act, 35 P.S. § 7601 et seq.

Disease Prevention and Control Law of 1955, 35 P.S § 521.1 et seq.

Right-To-Know Law, 65 P.S. § 67.101 et seq.

Mental Health Procedures Act (50 P.S. §7111 et seq.)

Mental Health Treatment Regulations (55 Pa. Code §5100.31 et seq.)

Drug and Alcohol Abuse Control Act (71 P. S. §1690.101 et seq.)

Breach of Personal Information Notification Act (73 P. S. §2301 et seq.)

Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191, 104th Congress.

The Privacy, Security, Breach Notification, and Enforcement Rules set forth in 45 CFR Part 160 and Part 164.

Health Information Technology for Economic and Clinical Health Act, Public Law No. 111-05, 111th Congress (2009).

Federal substance abuse treatment confidentiality law and regulations codified as 42 USC 290dd-2 and 42 CFR Part 2

Identity Theft Prevention Rules under 16 CFR §681.1

[REMAINDER OF THIS PAGE IS BLANK]