



Philadelphia Department of Public Health CONFIDENTIALITY POLICY Q&A – July 2014

This document provides an overview of the Philadelphia Department of Public Health's (PDPH) Confidentiality Policy. It does not address every issue that PDPH staff may encounter with regard to confidential information. Please be sure to complete confidentiality training, review the entire confidentiality policy, and talk with your supervisor or Division's Confidentiality Liaison if you have questions.

1. Where can I review the Confidentiality Policy?

The Confidentiality Policy is available online at: <http://citynet.phila.gov/health>.

2. Who makes sure that the Confidentiality Policy is implemented and followed?

Each PDPH employee is responsible for understanding the Confidentiality Policy and following its requirements. The Department's Confidentiality Officer is responsible for oversight, implementation, and evaluation across the Department. Each Division/Office has a designated Confidentiality Liaison who works with the Confidentiality Officer to ensure that staff within that Division are trained and aware of appropriate use of Division-specific confidential information. The PDPH Office of Human Resources assists with policy development and tracks completion of training.

3. How do I coordinate my mandatory Confidentiality Policy training?

Group in-person trainings will be available periodically, and an online self-study will also be available at <http://citynet.phila.gov/health>. If you are a new hire, you should receive an e-mail within two weeks concerning attendance at an upcoming training session. Please talk to your supervisor or Division's Confidentiality Liaison if you have not received training.

4. What is the purpose of the Confidentiality Policy?

The Confidentiality Policy helps to protect the privacy of people whose confidential information is collected, used, and/or shared by the Philadelphia Department of Public Health (PDPH). The Confidentiality Policy is also a requirement for maintaining Public Health Accreditation.

5. What is confidential information?

Confidential information includes any information about an individual that enables identification of that person. It includes an individual's name and address but can also include demographic, health, and service-related information that may be used to identify that person. For example, if you have the age, race, gender, and health conditions for an individual and also have information about his/her participation in a particular PDPH program, that combination of information may be enough to identify the person. Therefore, that information would be considered confidential.

Confidential information is not just paper-based or electronic information, but it can also be in oral, visual, or pictorial forms. For purposes of the Confidentiality Policy, confidential information does not include information collected by PDPH's Office of Human Resources (OHR). OHR follows a separate policy regarding confidentiality.

6. What are some of the most important things I have to do to protect confidential information?

- Do not share your computer passwords.
- Cover any paper-based confidential information when others are present.
- Safely put away confidential information when it is unattended.
- Lock your computer and any electronic devices when they are unattended.
- Follow current protocols for password protection and encryption.
- Unless otherwise approved, electronic confidential information may only be stored on Department-owned servers and devices.

7. Am I allowed to share confidential information with coworkers in the Department?

You may share confidential information with coworkers in the Department if it is necessary to meet the objectives of a PDPH program/initiative. You cannot share information with a coworker if s/he does not need that information for work-related purposes. If you have any questions, please talk with your supervisor or Division's Confidentiality Liaison.

When sharing confidential information, you should send that information using appropriate methods. See question #9 for details.

8. Am I allowed to disclose confidential information to people outside of the Department?

Disclosing confidential information to people or entities outside of the Department requires approval. This approval can come in various forms.

For information that is regularly shared with other agencies, your Division/Office may have a standing approval. Please check with your supervisor or Confidentiality Liaison. Examples include:

- Medical Examiner's Office: Sharing of autopsy data with law enforcement
- Disease Control: Sharing of communicable disease data with state and federal public health agencies
- Ambulatory Health: Sharing of billing information with insurance companies

Without a standing approval, you must work with your Confidentiality Liaison to seek an approval. This may be needed for program operations, service provision, or research. In some cases, you may need authorization from the individual whose information you are sharing.

When sharing confidential information, you should send that information using appropriate methods. See question #9 for details.

9. How can I send confidential information to another person or organization?

You may send confidential information by hand delivery, fax, inter-office mail, U.S. Mail, delivery or courier service, phone, or electronically. Of note, sending confidential information by email requires approval of your Confidentiality Liaison and the Confidentiality Officer. Below are key considerations according to the chosen delivery method.

Hand delivery	Ensure that the confidential information is not visible during transport.
Fax	Verify the recipient; inform the recipient of your intention to send a fax; include confidentiality cover sheet; remove original and confirmation from machine and keep record.
Inter-office mail	Verify recipient; send in a security envelope marked "Confidential".
Mail or courier	Verify recipient; use security envelope marked "Confidential"; send by registered or certified mail whenever feasible.
Phone	Confirm identity before revealing confidential information.
Electronic	Use password-protected (and encrypted, as feasible) Department networks, servers, flash drives, CDs/DVDs.
Email	Requires approval of Confidentiality Liaison and Officer.

10. How do I dispose of Confidential Information properly?

For paper-based confidential information, proper disposal means shredding (preferably with a high-quality crosscut shredder) at the office. For electronic confidential information, destruction must be done with appropriate file swiping/cleaning software. Please work with your Confidentiality Liaison regarding disposal of electronic confidential information.

11. What should I do if I believe someone has not complied with the Confidentiality Policy?

If you suspect that you or someone else has violated the Confidentiality Policy, you must report the non-compliance within one business day to Health-Confidentiality@phila.gov. Failure to report may make you subject to disciplinary action.

12. What other privacy and data security rules apply to me?

Ambulatory Health Services, the Public Health Laboratory, and the Philadelphia Nursing Home are also subject to **HIPAA** and the Department's **HIPAA Policy**.

The AIDS Activities Coordinating Office, the Division of Disease Control, and the Office of Human Resources maintain additional confidentiality requirements specific to their divisions.

The nature of your work may also make you subject to various laws, identified in Section VI of the Confidentiality Policy. Your supervisor will inform you of additional rules applicable to you.

13. Whom should I contact with questions?

Please contact your supervisor or Confidentiality Liaison. Questions can also be sent to Health-Confidentiality@phila.gov.