

## POLICY AND PROCEDURE MANUAL

---

### 1. GENERAL ADMINISTRATION.

---

#### 1.07 Confidentiality of Participant Records.

---

##### A. POLICY:

The PA WIC Program shall respect and protect participant Protected Health Information (“PHI”) and WIC confidential information (collectively, hereinafter “information”) and release only the minimum information necessary to carry out the purposes of any legitimate request for release of information. In accordance with 7 C.F.R. §246.26 of the Federal WIC Regulations, confidential participant information is any information about an applicant or participant that individually identifies an applicant or participant and/or family member(s).

##### B. PROCEDURE:

###### 1. Participant Information and Confidentiality Protections

Participation in WIC is voluntary but requires participant disclosure of intimate details of daily life in order to fully assess participant needs. In order to assure trust and bolster confidence that will encourage and facilitate involvement in the Program leading to optimal benefit, the following shall apply:

###### a. WIC participants shall be afforded the following protections:

- (1) Program staff is responsible for employing reasonable measures to safeguard PHI from any intentional or unintentional use or disclosure that is in violation of 7 C.F. R. §246.26 of the Federal WIC Regulations. Information to be safeguarded may be in any medium, including paper, electronic, oral, and/or visual representations of confidential information.
- (2) WIC employees are responsible for safeguarding information and must take the following safeguards to protect information in the workplace and at workstations:

###### (a) Paper / hard copy document files must:

1. Be retained in appropriate secure areas or containers, such as lockable desks, file rooms or approved open area storage systems.
2. Be secured at all times when not in use and during non-office hours.
3. Be retained as indicated on the Bureau File Retention Schedule with those documents authorized for destruction being shredded by Bureau administrative staff or placed in secured containers provided by a shredding contractor if so employed and emptied regularly by the vendor.
4. Be protected from view of unauthorized individuals, including documents on desks, fax machines, photocopy machines, portable electronic devices (e.g., laptop computers, BlackBerrys, iPad's, Smartphones, etc.), computer printers, and in common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.).

###### (b) Verbal or oral communications containing information must exercise reasonable precautions to protect the privacy of confidential information, regardless of where the discussion occurs and consider level of risk, including:

1. Low Risk: interview rooms, enclosed offices and conference rooms.
2. Medium Risk: employee-only areas, telephone and individual cubicles.
3. High Risk: public areas, reception areas and shared cubicles housing multiple staff where clients and other employees who may not be part of the covered entity are routinely present.

**POLICY AND PROCEDURE MANUAL**

---

1. GENERAL ADMINISTRATION.

---

1.07 Confidentiality of Participant Records.

---

- (c) Visual communications containing information must be shielded from unauthorized disclosure, including:
  - 1. Use of polarized screens or other computer screen overlay devices as needed that shield information on the display from unauthorized view
  - 2. Placement of computers such that displays are out of the visual range of unauthorized view
  - 3. Clearing information from the screen when not actually being used
  - 4. Using screen savers or program screens that automatically go blank when not in use
  - 5. Locking-down computer work stations when not in use
  - 6. Clearing the copier memory as needed
  - 7. Other effective means as available
- (d) Other administrative safeguards must be exercised as appropriate, including:
  - 1. Applying user level security protocols that allow DOH employees and workforce members to only have access to applications that may contain information on a need-to-know basis as defined by job title and position description
  - 2. Requiring Bureau Director or designee approval to add or delete user level rights outside of approved user group assignment to access certain applications or certain screens of applications, etc., when it is determined that an employee or workforce member has a need-to-know of otherwise restricted information
  - 3. Assuring that managers are enforcing the "Minimum Necessary Information" standard and allowing staff to only access enough information to do their jobs
  - 4. Restricting the collection and storage of participant social security numbers
  - 5. Promoting an environment where managers and supervisors foster a secure atmosphere and enhance the belief that protecting the privacy of information, and all confidential information, is important and necessary
- (3) Local agency (LA) staff shall send any requests for records pertaining to court orders or subpoenas to the State Agency (SA) for review by Department of Health legal counsel.
- (4) WIC staff shall not share or provide non-WIC entities access to participant information either interagency or intra-agency through the use of a centralized database without a specific Memorandum of Understanding between the programs involved outlining the purpose of information sharing, the specific information needed and the limitations of information use and re-disclosure, which shall be reviewed and approved by the SA.
  - (a.) Persons requesting release of participant information shall be informed that LA personnel can neither confirm nor deny the individuals' status and be informed of WIC disclosure limitations.
  - (b.) Joint eligibility forms shall only be used for intake procedures and shall not constitute grounds to authorize ongoing sharing of information.
  - (c.) Information obtained from a third party shall not be released.
  - (d.) LA staff shall obtain a signed Consent to Release of Information form from endorsers prior to contacting or referring their names to non-WIC agencies for services, except in the case of mandatory child abuse reporting to Children and

## POLICY AND PROCEDURE MANUAL

---

### 1. GENERAL ADMINISTRATION.

---

#### 1.07 Confidentiality of Participant Records.

---

Youth Services. Endorsers shall be informed that their WIC benefits will not be affected by agreeing or refusing to sign Consent to Release of Information forms.

- (e.) Blanket release forms that would allow “as needed” or “on-going” exchange of information between the Program and participant physicians, social service agencies or any other third party is expressly forbidden.
  - (f.) Children who are adopted shall receive a new participant identification number. Refer to Standard Operating Procedures (SOP) under “Handling Adoption Records” for instructions on separating the former record from the new adoptive child record.
2. Minimum Necessary Release of Information
- a. Program staff will assure that the minimum necessary amount of information is used and disclosed by:
    - (1) Assessing the task at hand and identifying, requesting and/or supplying the specific information required to accomplish the intended purpose of the use, disclosure, or request.
    - (2) Information that is not required to achieve the specific purpose of the requested release will either be omitted entirely or redacted to prevent unnecessary release.
  - b. When the SA permits the release of information to another entity, Program staff shall apply the minimum necessary policy when:
    - (1) Responding to public officials permitted access under 45 C.F.R §164.512 (NOTE: a “public official” is any employee or workforce member of a government agency who is authorized to act on behalf of that agency in performing the lawful duties and responsibilities of that agency).
    - (2) The information is requested by another entity that is a “covered entity” under the HIPAA Privacy rules (i.e. “covered entity” is a health plan, a health care provider who conducts electronic transactions, or a health care clearinghouse).
    - (3) The information is used or the disclosure is required for compliance with the HIPAA Transaction Rule.
    - (4) The disclosure to or requests for information are by a health care provider for treatment.
    - (5) The information is requested by a member of a “covered entity”, or is a business associate of the “covered entity”, for the purpose of providing professional services.
    - (6) A person requesting the information for research purposes has been authorized by the DOH to use the specific data requested for the stated research purposes. Such authorization shall be reviewed and approved by the Program/Bureau Director, the Office of Legal Counsel, as well as the Department Research Review Team.
  - c. Restrictions of “minimum necessary policy” do not apply to the following circumstances:
    - (1) Disclosures made to the individual about his or her own protected information
    - (2) Uses or disclosures authorized by the individual that are within the scope of the authorization
    - (3) Disclosures made to the USDA Food and Consumer Services
    - (4) Pennsylvania Auditor General
    - (5) Pennsylvania Inspector General
    - (6) Comptroller General of the United States

## POLICY AND PROCEDURE MANUAL

---

### 1. GENERAL ADMINISTRATION.

---

#### 1.07 Confidentiality of Participant Records.

---

- (7) National, State and local WIC staff, managers and administrators
- (8) Auditors conducting federally mandated audits of a LA
- (9) United States Department of Health and Human Services (DHHS) in accordance with subpart C of part 160 of the HIPAA Privacy Rule
- (10) Uses or disclosures that are required by law

#### 3. Enforcement

- a. All DOH supervisors and managers are responsible for enforcing this policy. Individuals who violate this policy will be subject to appropriate and applicable disciplinary action, up to and including termination or dismissal.
- b. All LAs are responsible for enforcing this policy. Individuals who violate this policy will be subject to appropriate and applicable disciplinary action, up to and including termination or dismissal.

#### 4. Reporting Child Abuse to Child Protective Services

- a. Staff must report all suspected or observed child abuse or neglect **immediately** by telephone to the statewide toll-free ChildLine 1-800-932-0313. Staff may not make an independent determination of whether to report. Staff must also inform the LA WIC Director that a report has been filed with ChildLine.
- b. Within 48 hours of reporting to ChildLine, the reporter makes a written report, on forms provided by the Department of Human Services, to the Child Protective Services in the county where the suspected abuse occurred. Blank report forms can be obtained from the local county agency and kept on-site.
- c. The staff person reporting the abuse or neglect documents in the participant's file that suspected abuse was reported.
- d. The identity of the person filing the report or cooperating in the investigation is considered confidential and will not be released to the subject of the report. **EXCEPTION:** The Secretary of the Department of Human Services has the authority to release the identity of the person filing the report if the Secretary finds that the release will not harm the safety of the person filing the report.

---

#### References(s):

- 1. WIC Regulations: 7 CFR, Part 246.26(d).
- 2. PA Child Protective Services Law 23 PA. C.S.A. §§6301-6385.
- 3. 55 PA Code §§34901.1-3490.210.
- 4. FNS Instruction 800-1 dated March 30, 1990.
- 5. USDA Memo 93-040.
- 6. USDA Memo 94-070.

---

#### Policy and Procedure Status:

- 1. This P&P supersedes P&P 1.10 dated June 11, 2012.
- 2. This P&P supersedes P&P 1.13 dated March 19, 2004.