Toledo-Lucas County Health Department Policy

Personally Identifiable Information Policy

Original Effective Date:	Review / Revision Date:	Board of Health Resolution:
May 24, 2018		2018.05.065

Maintenance Steward: Privacy Officer **History:** ☒ New ☐ Revised ☐ Archived

Organizational Scope:

☒ Full Agency ☐ Administration ☐ Community Services ☐ Environmental Health ☐ Health Services

Frequency of Review:

☒ Annually ☐ Biennially ☐ 5 Years ☐ As Needed ☐ Other:

Location:

G-Drive: G: → Users → Common → Policies & Procedures

Website: www.lucascountyhealth.com/employee-login/

Hardcopy: TLCHD Policies & Procedures Manual, HR Office

Archived Version(s):

Requisite Signatures

☒	Board of Health President	Date: 24 May 2018
☒	Health Commissioner	Date: 05-24-18
☒	Director of Administrative Services (Vacant)	Date
☒	Director of Environmental Health & Community Services	Date: 24 May 2018
☒	Director of Health Promotion & Policy Integration	Date: 5/24/2018
☒	Director of Health Services	Date: 5/24/18
☒	Human Resources Administrator	Date: 5-24-2018

Personally Identifiable Information Policy

I. Policy

It is the policy of the Toledo-Lucas County Health Department to protect the personally identifiable information (PII) of employees and the public by ensuring the proper use, dissemination, and maintenance of PII collected in the course and scope of normal operations.

II. Scope

This policy applies to all officials, employees, or other representatives of the Toledo-Lucas County Health Department.

III. Purpose

To ensure that any PII collected by, or shared with TLCHD is done so in compliance with all state and federal regulations and information security best practices. This policy outlines the means through which the department uses, stores, secures, accesses, and shares PII for employees and clients.

IV. Background

The Health Department is required to protect PII under the Code of Federal Regulations (CFR) and the Ohio Revised Code (ORC).

Pursuant to **2 CFR 200.79**:

> *Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example,* ***first and last name, address, work telephone number, email address, home telephone number, and general educational credentials****. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.*

Pursuant to **2 CFR 200.82**:

*Protected PII means an individual's **first name or first initial and last name** in combination with any one or more of types of information, including, but not limited to, **social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts**. This does not include PII that is required by law to be disclosed.*

Pursuant to **2 CFR 200.303**:

The non-federal entity must:

a. *Establish and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statues, regulations, and the terms and conditions of the federal award.*
b. *Comply with Federal statues, regulations, and the terms and conditions of the Federal awards.*
c. *Evaluate and monitor the non-federal entity's compliance with statutes, regulations, and the terms and conditions of federal awards.*
d. *Take prompt action when instances of non-compliance are identified including noncompliance identified in audit findings.*
e. *Take reasonable measures to safeguard protected PII and other information the federal awarding agency or pass-through entity designates as sensitive or the non-federal entity considers sensitive consistent with applicable federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.*

Additionally, the Health Department conforms to the *Confidentiality Statutes* under ORC sections *1501-8-04*, *3701-75-04*, and *4501-55-05*, and all provisions of the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*.

Many of the following provisions are also stipulated in the ***Computer, Network, & Internet Acceptable Use*** and the ***Department Issued Equipment*** policies, and these policies should be used as additional references for the proper use, protection, and dissemination of PII.

V. Collection of PII

A. TLCHD will collect information about an employee that is necessary for the treatment, payment, and health care operations of its employee benefits program, payroll processes, and for other administrative requirements as necessary.

1. TLCHD may receive information from various sources including transactions with health care providers, other insurers, third-party administrators, vendors, consultants, and other Lucas County representatives.

2. This includes information about the employee and the employee's dependents in order to provide insurance coverage or requested services.

B. TLCHD will collect personally identifiable information from members of the public that is necessary for the provision of public health programs and services.

VI. Accessing, Using, and Securing PII

A. Staff may access, use, or share PII only to the extent it is both authorized and necessary to fulfill assigned job duties.

1. Passwords may not be shared; providing access to another individual, either deliberately or through failure to secure access is expressly prohibited.
2. Employees must lock their workstation/computer or log off when the device is unattended to prevent unauthorized access to PII.

B. Staff shall not share any individually identifiable information with any unauthorized party for any reason.

1. Disciplinary action up to and including termination may result from improper access, use, storage, or dissemination of PII or protected health information (PHI).

C. All physical files that contain protected PII must be secured within a locked file cabinet or room when not being actively accessed, used, or modified.

1. During environmental or operational changes that could affect the security of PII, staff shall routinely monitor and evaluate procedures to adequately protect PII in accordance with all federal and state laws and regulations.

D. Protected PII is not to be downloaded, stored, or transported on personal or unauthorized workstations or mobile devices (including removable media) or on systems outside the protection of the department.

E. PII should never be sent through any form of insecure electronic communication.

F. Computers should be secured both physically and digitally; staff should secure computers by returning to the log-in screen when away from their work station to prevent data theft or the release of sensitive information; staff may consider placing laptops and other peripheral equipment in desk drawers or cabinets if they will be absent from their workstation for a prolonged period of time.

G. When in the field, employees shall take the following precautions to minimize the risk of theft or loss of PII on any medium:

1. When possible, issued equipment and sensitive paperwork should be kept on or near the staff member's person at all times;
2. When not physically with a staff member, any device or medium with PII should be locked in the trunk of a vehicle within the control of, or accessible to, health department staff, or secured on-site (e.g., manager's office, locker, etc.); If a trunk is not available, computers and other issued equipment should be placed out of sight (e.g., under a seat or otherwise hidden);
3. Vehicles should be locked at all times.

VII. Dissemination of PII

A. TLCHD will use and disclose PII in accordance with all legal statutes for the proper management and administration of its programs and services, for payroll processing, its benefits program, and all other human resource functions requiring the collection, dissemination, or use of PII.

B. TLCHD will make every reasonable effort to limit the disclosure of PII to the minimum necessary to accomplish the intended purpose.

C. Permissible Disclosures of PII

1. Workers' Compensation disclosures or similar programs that provide benefits for work related injuries or illness without regard to fault.
2. Disclosure necessary to prevent or lessen serious threat to the health or safety of personnel or the public.
3. Disclosures of PHI in response to a court or administrative order, subpoena, or law process; to identify a decedent or determine the cause of death.
4. Disclosures of PHI on research projects; for the oversight of the health care system, government benefit programs; Armed Forces; national security or intelligence activities.
5. Disclosure of PHI to Health and Human Services to investigate or determine TLCHD's compliance with the HIPAA Privacy Rule.

D. Other than as permitted by law, TLCHD will not share employee PII or PHI with non-affiliated third parties without giving the employee an opportunity to state what they do not want TLCHD to share.

VIII. Breach Reporting and Actions

A. Employees with access to PII through any medium shall not wait for confirmation that a breach has occurred before reporting a potential breach to the agency.

1. Any real or suspected disclosure of protected PII data must be reported to the Health Commissioner and Privacy Officer within 12 hours of discovery (e.g., misplacing a paper report, loss of a laptop, mobile device, or removable media containing PII; accidental email of PII, possible virus or malware infection of a computer containing PII).

2. Even if it is believed that the misplaced, lost, or stolen information can or will be recovered, it must be reported without delay. Unnecessary delay may undermine the agency's ability to apply preventative and remedial measures to protect the PII or reduce the risk of harm to potentially affected individuals.

B. When a potential or actual breach of PII has been reported, the Privacy Officer shall consider the following factors for assessing the risk of harm to potentially affected individuals:

1. Nature and sensitivity of the PII potentially compromised by the Breach, including the potential harms that an individual could experience from the compromise of that type of PII;
2. Likelihood of Access and Use of PII, including whether the PII was properly encrypted or rendered partially or completely inaccessible by other means;
3. Type of Breach, including the circumstances of the breach, as well as the actors involved and their intent;
4. Data Elements, including an analysis of the sensitivity of each individual data element as well as the sensitivity of all the data elements together (see ***Appendix B***);
5. Context, including the purpose for which the PII was collected, maintained, and used;
6. Private Information, including the extent to which the PII, in a given context, may reveal particularly private information about an individual;
7. Vulnerable Populations, including the extent to which the PII identifies or disproportionately impacts a particularly vulnerable population; and
8. Permanence, including the continued relevance and utility of the PII over time and whether it is easily replaced or substituted.

C. The Privacy Officer will complete a Breach Incident Report and will work with agency leadership to determine the best course of action to remediate potential harm and to prevent or reduce the risk of a future breach (see ***Appendix A*** for a Breach Incident Report template).

IX. Maintenance

A. Review

1. The *Personal Identifying Information* policy is to be reviewed annually to ensure compliance with both agency and accreditation standards.

B. Revision

1. All changes made to this policy are to be noted on the **Record of Change**. Substantial changes will require renewed signatures from all applicable parties. This includes changes to the intent, scope, procedures, or policy statement.

2. Changes in style, format, grammar or minor error correction will not require renewed signatures but must be indicated on the Record of Change.

X. Glossary

A. <u>Personally Identifiable Information (PII)</u>: Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

B. <u>Protected Personally Identifiable Information (Protected PII)</u>: An individual's first name or first initial and last name in combination with any one or more of types of information including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII that is required by law to be disclosed.

C. <u>Public Health Authority</u>: An agency or authority of the United States, a State, territory, a political subdivision of a State or territory, or an Indian Tribe; a person or entity acting under a grant from or in contract with such a public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Record of Change

(Required for all policies)

Date of Change	Changes Made By	Changes Made/Notes	Approved By

Appendix A: Breach Report Template

TLCHD Breach of Personally Identifiable Information (PII) Report					
This form is to be completed in the event of a suspected or actual breach of PII is reported. The Privacy Officer will complete this report and submit it to agency leadership to determine the appropriate actions for the remediation of any potential, perceived, or realized harm resulting from the release, loss, or misuse of protected PII.					
Initial Report	*Select Date*	**Updated Report**	*Select Date*	**After Action Report**	*Select Date*

1. General Information:

Date of Breach	**Date Breach Discovered**	**Date Breach Reported**
Select Date	*Select Date*	*Select Date*

Location of Breach	*Where Did the Breach Occur?*		
# Individuals Affected	*# Affected*	**Were Affected Parties Notified?**	☐Yes ☐No *If Yes, Date:* *Select Date*

Reported By	**Breach Involved**	**Type of Breach**	**Cause of Breach**
Select from List	*Select from List*	*Select from List*	*Select from List*

Name	*First & Last Name*	**Supervisor**	*First & Last Name*	☐ N/a
Email	*Official Email*	**Email**	*Official Email*	
Phone #	*Official Phone*	**Phone #**	*Official Phone*	

2. Summary of the Breach:

Do not include PII or classified information. Summarize the facts or circumstances of the theft, loss, compromise, or unauthorized use of PII as currently known, including:
(a) A description of the parties involved in the breach;
(b) The data elements (type) involved in the breach (descriptors only, not the actual PII)
(c) The physical or electronic storage location of the information at risk;
(d) If steps were immediately taken to contain the breach;
(e) Whether the breach is an isolated occurrence or a systematic problem;
(f) Who conducted the investigations of the breach, if applicable; and
(g) Any other pertinent information.

3. Actions taken :

Do not include PII or classified information. Summarize the actions taken in response to the breach, including:
(a) Actions taken;
(b) Preventative actions to limit recurrence;
(c) Lessons Learned.

Appendix B: Data Elements

Data Elements and Information Types

This appendix includes examples of data elements and information types that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Identifying Numbers

Social Security Number	Truncated or Partial Social Security Number
Driver's License Number	License Plate Number
DEA Registration Number	File/Case ID Number
Patient ID Number	Health Plan Beneficiary Number
Student ID Number	Federal Student Aid Number
Passport Number	Alien Registration Number
Employee Identification Number	Professional License Number
Taxpayer Identification Number	Personal Bank Account Number
Credit/Debit Card Number	Personal Device Identifiers or Serial Numbers
Vehicle Identification Number	Personal Mobile Number

Biographical Information

Name (including nicknames)	Gender	Race
Date of Birth	Ethnicity	Nationality
Country of Birth	City or County of Birth	Marital Status
Citizenship	Immigration Status	Religion/Religious Preference
Home Address	Zip Code	Home Phone or Fax Number
Spouse Information	Sexual Orientation	Alias
Group/Organization Membership	Military Service Information	Professional/personal references
Personal Email Address	Business Email Address	GPS/Location Data
Personal Financial Information	Employment Information	Children Information
Education Information	Resume or Curriculum Vitae	Mother's Maiden Name

Biometrics/Distinguishing Features/Characteristics

Fingerprints	Palm Prints	Vascular scans
Retina/Iris Scans	Dental Profile	Scars, marks, tattoos
Hair Color	Eye Color	Height
Video Recording	Photos	Voice/Audio Recording
DNA Sample or Profile	Signatures	Weight

Medical/Emergency Information

Medical/Health Information	Mental Health Information	Disability Information
Workers' Compensation Information	Patient ID Number	Emergency Contact Information

Appendix B Data Elements

Device Information

Device settings or preferences (e.g., security level, sharing options, ringtones)	Cell tower records (e.g., logs, user location, time, etc.)	Network communication data

Specific Information/File Types

Taxpayer Information/Tax Return Information	Law Enforcement Information	Security Clearance/Background Check Information
Civil/Criminal History Information/Police Record	Academic and Professional Background Information	Health Information
Case Files	Personnel Files	Credit History Information