City of El Paso

Personally Identifiable Information Policy

Prepared by:
Community + Human Development
EFFECTIVE April 30th, 2020

Intentionally Left Blank

Contents

1. Application of Policy

The Department of Community and Human Development (DCHD) Personally Identifiable Information Policy ("PII Policy") sets forth the minimum standards to protect personally identifiable information ("PII"). These standards are cast as practices herein; they represent the set of expectations against which policy compliance will be assessed. Further obligations imposed by law, regulations, contracts, or other institutional policies also apply.

All DCHD staff are required to adhere to this PII Policy.

2. Policy

It is DCHD policy to protect the privacy of personally identifiable information that is within its control. PII is information that can be used to identify an individual, whether on its own or in combination with other personal or identifying information that is linked or linkable to an individual. PII can be that of current and prospective workforce members, sub-recipient agencies, advisory committee members, vendors, visitors, and others.

Federal and state information privacy laws require the DCHD to protect certain elements of PII, often because of the sensitivity of the data and/or its potential for misuse for fraudulent activities or other forms of identity theft. These laws may require the DCHD to self-report to the state or federal government and/or provide notice to affected individuals if the security of certain PII is breached.

The following table provides examples of different types of PII:

Examples of PII that may require legal notification of a breach	**Examples of Other Legally Protected PII that is considered Sensitive/Confidential**	**Examples of Other Forms of PII with the potential for misuse**
Social Security numbers	Sub-Recipient Reimbursement Records	Date of Birth
Credit card numbers	Schedules	User credentials
Financial account information	Banking and personal financial information related to student financial aid that does not include account information (e.g. credit scores)	Partially redacted PII (e.g., last 4 digits of SSN)
Driver's license numbers	Employee records (e.g. human resources)	Employee ID numbers
	Records of an administrative hearing	

A given element of PII may be protected under more than one federal or state law.

The PII elements below are not necessarily considered private, but combining these elements with other PII may have privacy implications.

Examples of Other PII that may be misused if combined with other PII or aggregated
Address
Phone number
Email address
Employee ID
Employee directory information in which the employee has not opted out (like that above, but also dates and photos)

3. Protection and Handling of PII

The following requirements apply to PII in paper records, electronic records, and in oral communications, as well as any aggregation of PII in an electronic format (e.g., databases, webpages, e-mail, spreadsheets, tables, and file-sharing services such as OneDrive).

1. General -- In addition to complying with all applicable legal requirements, DCHD further limits the collection, use, disclosure, transmission, storage and/or disposal of PII to that which fulfills the DCHD mission.

2. Safeguards -- To protect PII against inappropriate access, use, disclosure, or transmission, DCHD requires appropriate administrative, technical, and physical safeguards. Divisional leadership is responsible for documenting security controls and safeguards and risk management consistent with the Information Technology Security policy. Examples of physical safeguards include storing documents containing PII in secured cabinets or rooms and ensuring that documents containing PII are not left on desks or in other locations that may be visible to individuals not authorized to access the PII.

3. Collection –Collected data should be appropriate for the intended authorized use, and collection should be conducted according to best practice and legal requirements for the type and purpose of data collected. Since the collection process itself can potentially lead to unintended PII disclosure, considerations of confidentiality in collection and recording should be explicitly addressed.

4. Minimization -- All members of the DCHD staff are responsible for minimizing the use of PII (including redaction of financial account information, use of less sensitive substitutes such as partial SSN) and minimizing aggregations of PII. The risk of unauthorized disclosure of or access to PII increases with the amount of data. All DCHD staff are responsible for ensuring that the number and scope of physical and electronic copies and repositories of PII are kept to the minimum necessary and only for the period where a valid business need for the information exists.

5. Permitted Use within DCHD -- Only individuals within DCHD who are permitted under law, regulation and City policies and have a legitimate "need to know" are authorized to access, use, transmit, handle or receive PII, and that authorization only extends to the specific PII for which the relevant individual has a legitimate "need to know" to perform his or her job duties.

6. Permitted Disclosure to Third Parties -- DCHD may release PII to third parties only as permitted by law/regulation and under the City of El Paso Information Technology Department policy. Third-party contractors to whom DCHD is disclosing PII must be bound by agreements with appropriate PII safeguarding and use provisions.

7. Oral Communications -- Only authorized individuals may engage in oral communications involving PII. Caution is required in all oral communications involving PII, and oral communications involving PII may not take place in any location where the communication may be overheard by an individual not authorized to access the PII.

8. Storage of PII -- PII may be stored only as necessary for the DCHD mission and permitted under the City of El Pas Records and Retention policy. Divisional leadership is responsible for providing guidelines around where information can be scanned/stored (e.g. in hardcopy, on shared drives, on other media/devices) and how long information may be retained before requiring deletion or destruction). In addition, divisional and entity leadership is responsible for maintaining an up-to-date inventory of stored or maintained documents, files, databases and data sets containing PII, and their contents, and requiring encryption of PII stored on mobile devices, media, or other at-risk devices such as public workstations.

9. Transmission of PII -- PII may not be transmitted to external parties outside the DCHD (e.g. via mail, fax, e-mail, instant messaging) without appropriate security controls. Generally, such controls include encryption and authentication of recipients (e.g., password protection of files; verifying fax numbers; cover sheets; marking documents as confidential). Great care is to be taken to ensure that e-mails are sent only to intended recipients.

10. Disposal -- PII must be destroyed and rendered unreadable before disposal. For example, this may include shredding papers or wiping electronic files.

11. Training -- Each DCHD division is responsible for ensuring that its personnel completes appropriate training on the City of El Paso Information Technology privacy policies, before accessing, using, transmitting, handling, or receiving PII.

4. Enforcement and Exceptions

Each DCHD division is responsible for ensuring that its PII handling practices are consistent with the practices described in this PII Policy. This responsibility includes the entire set of activities within *enforcement*, including surveillance and detection of non-compliance with the Policy, the identification and implementation of the individual and organizational-level corrective actions, and (where appropriate) the imposition of sanctions. As a practical matter, it may be occasionally necessary and appropriate to diverge from these best practices to advance the City of El Paso's mission. In such cases, it is the responsibility of the head of the department to ensure that such divergences are approved, documented, and communicated to stakeholders.

5. Breaches of the Privacy of PII

Known or suspected violations of this policy should be reported promptly. Any incidents that have the potential to damage departmental and/or the City of El Paso network operations should be reported immediately. Violators of this policy may be subject to criminal and/or civil penalties and to disciplinary action, up to and including termination.

In the event of a known or suspected privacy breach, contact for the City of El Paso Information Technology Department, at (915) 212-0072, City Attorney Office, (915)-212-0034.

Related Policies:

- *Privacy Policy – Information Technology Department*
  - *https://www.elpasotexas.gov/privacy-policy*
- *Security Policy – Information Technology Department*
  - *https://www.elpasotexas.gov/security-policy*