



Subject: Data Privacy Policy
Date Issued: May 13, 2014
Issued by: Information Technology Governance Committee
Approved by: The County of Monterey Board of Supervisors
Applies to: All County Officials, Employees and Affiliates

3. DATA PRIVACY POLICY

3.1. POLICY PURPOSE

To establish practices for protecting the privacy of personal and/or Personally Identifiable Information that may be collected through the use of the County's information technology resources.

3.2. POLICY SCOPE

This policy applies to all County officials, employees and affiliates.

3.3. DEFINITIONS

- 3.3.1. Affiliates – Includes but is not limited to, third party contractors, volunteers, advisory and other committee and commission members, vendors, or others associated with the County in order to accomplish County business.
- 3.3.2. Cookies – a piece of text describing user preferences and choices, typically stored in a small file on the user's computer hard drive as a result of accessing a web site and interacting with it via web browser software.
- 3.3.3. Personally Identifiable Information (PII) – personal data that includes names, identification numbers (social security numbers, driver's license numbers, account names, passwords, etc.), post and e-mail addresses, phone and facsimile numbers, billing information, medical records, vehicle information such as vehicle identifications numbers, and complaint information.

3.4. POLICY DESCRIPTION

- 3.4.1. Monterey County and its departments shall implement data privacy and confidentiality practices that meet the requirements of state and federal legislation and regulation, as they may be amended and supplemented from time to time, including (but not necessarily limited to) the following laws:

- 3.4.1.1. Lanterman-Petris-Short Act (LPS) of 1969

- 3.4.1.2. The Fair Credit Reporting Act (1970)
- 3.4.1.3. Privacy Act of 1974
- 3.4.1.4. Family Education Rights and Privacy Act (1974)
- 3.4.1.5. Right to Financial Privacy (1978)
- 3.4.1.6. Confidentiality of Medical Information Act (CMIA) of 1979
- 3.4.1.7. Privacy Protection Act of 1980
- 3.4.1.8. Cable Communications Policy Act of 1984
- 3.4.1.9. Electronic Communications Privacy Act (1986)
- 3.4.1.10. Patient Access to Health Records Act (PAHRA) of 1988
- 3.4.1.11. Driver's Privacy Protection Act of 1994
- 3.4.1.12. Communications Assistance for Law Enforcement Act of 1994
- 3.4.1.13. Telecommunications Act of 1996
- 3.4.1.14. Health Insurance Portability and Accountability Act (HIPAA) of 1996
- 3.4.1.15. Children's Online Privacy Protection Act (COPPA) of 1998
- 3.4.1.16. Financial Modernization Act (Graham-Leach-Bliley Act) (2000)
- 3.4.1.17. USA Patriot Act (2001)
- 3.4.1.18. SB 1386, the California Information Practices Act (2003)
- 3.4.1.19. The Payment Card Industry Data Security Standard (PCI DSS) (2004)
- 3.4.1.20. Patient Safety and Quality Improvement Act (2005)
- 3.4.1.21. DHCS Medical Data Privacy & Security Agreement (2007)
- 3.4.1.22. Genetic Information Nondiscrimination Act (GINA) 2008
- 3.4.1.23. Health Information and Technology for Economic and Clinical Health Act (HITECT) of 2009
- 3.4.1.24. Red Flag Program Clarification Act (2010)
- 3.4.2. County officials, employees, affiliates or others with access to PII through the County's information technology resources shall abide by this policy, hold any such information in confidence, and shall not use such information for any purpose other than to carry out the County business purpose they are charged with performing.
- 3.4.3. Monterey County shall not sell, rent, or lease PII to third parties. The County shall not share any PII with any outside party without first ensuring that the outside party has similar privacy policies in place. Exceptions include the following situations:
 - 3.4.3.1. Sharing the information, on an expedited basis, is in the vital interests of the subject of that information or some other person (e.g., health care information).
 - 3.4.3.2. Sharing the information is necessary to carry out law enforcement duties and responsibilities.
 - 3.4.3.3. Sharing the information is necessary for the establishment of a legal claim or defense.

- 3.4.3.4. Sharing the information is related to the provision of medical care or diagnosis.
- 3.4.3.5. The subject of the information has consented to sharing the information with third parties.
- 3.4.3.6. The information has been unambiguously made public by the subject of that information.
- 3.4.3.7. The information is mandated to be made available to qualified third parties by law or code (e.g., California State Elections Code).

3.4.4. Posting the Privacy Policy

- 3.4.4.1. County Departments shall post a summary privacy policy as it specifically applies to the information handled by their department. This should include providing notice as to what personal information is collected, used, and disclosed; what choices persons conducting business with the County have with regard to the business collection, use, and disclosure of that information; what access the public or others will have to that information; what security measures are taken to protect the information, and what enforcement and redress mechanisms are in place to remedy any violations of this policy.

3.4.5. Provide Adequate Security to Maintain Privacy

- 3.4.5.1. County Departments shall take all reasonable steps to ensure that PII is safe from unauthorized access, either physical or electronic. These steps will include at least the following:
 - 3.4.5.1.1. Maintain logs to properly track information and assure that data is only accessed by individuals authorized by the department.
 - 3.4.5.1.2. Perform at least an annual review of its written data security policies.
 - 3.4.5.1.3. Assure that officers, employees, affiliates and those with access to PII are properly trained on maintaining confidentiality.
 - 3.4.5.1.4. Store any such information in a secure environment (using features such as locks and electronic security).
- 3.4.5.2. County Departments shall use levels of encryption and authentication specified in the County's Information Security Standards for the transfer or receipt of health care information, social security numbers, financial transaction information (for example, a credit card number), or other sensitive or personally-identifiable information.
- 3.4.5.3. County Departments shall provide industry standard levels of security and integrity to protect data maintained on their computers, and shall contractually require all third parties and affiliates to provide and maintain similar and appropriate levels of security.

3.4.6. Respect Preferences Regarding Unsolicited E-Mail

- 3.4.6.1. County Departments shall enable those persons who do not wish to be contacted online with a means to opt out from future communications via electronic mail and shall maintain a "Do not contact" list.

3.4.7. Access and Correction

- 3.4.7.1. Any County Department that collects PII shall implement and maintain a process under which the collected information may be reviewed and factual

inaccuracies corrected upon request. The process shall include a means to authenticate the identity of an individual that requests access or correction. If review and/or correction are prohibited by law, an explanation of the prohibition shall be provided to authenticated individuals and a contact for further information will be provided, as well as a reference to the County's Information Technology Data Privacy Policy.

3.4.8. Computer Tracking and Cookies

- 3.4.8.1. The County web site shall not be designed or constructed to track, collect, or distribute personal information not specifically entered by visitors. Site logs may be used to generate certain kinds of non-identifying site usage data, such as the number of hits and visits to County sites. This information may be used for internal purposes by technical support staff to provide better services to the public and may also be provided to others; however the statistics shall contain no personally-identifiable information.
- 3.4.8.2. The County may use non-identifying cookies in support of easier web site navigation and access to forms. County web sites shall be designed to support access and use even if the user's browser is set to reject cookies. Cookies shall not be used to generate personal data, shall not read personal data from the user's machine, and shall not be connected to anything that could be used to identify the user.

3.5. **EXCEPTIONS**

Under rare circumstances, the County may need to vary from these policies. All such instances shall be approved in writing and in advance by the Director of Information Technology and/or the Chief Security and Privacy Officer. Disputed issues may be escalated to the Information Technology Governance Committee for final decision as necessary.

3.6. **ENFORCEMENT**

Violators of this policy may be subject to disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil. Similarly, contractors, affiliates and other third parties may be liable to a complaining party or the County for damages or penalties and to the County for indemnification and claim defense costs.