SACRAMENTO COUNTY	**Policy # 3200**
Subject: Electronic Data Access Policy	
Responsible Department: Technology	
Effective Date: 10/2000	**Revision Date:** 8/2018
Rami Zakaria **Chief Information Officer**	**Navdeep S. Gill** **County Executive**

1. Purpose:

This policy identifies County authority responsible for data classifications, delineates classification of County of Sacramento data, and defines access to each data classification.

2. Authority:

Chief Information Officer

3. Scope:

This policy applies to all County data and all County departments reporting to the County Executive.

4. Policy:

Responsibility

Department Directors have the authority to manage and classify data as public or confidential, and identify whether data contains personal and/or sensitive information. Department Directors are responsible for defining precautions and working with Department of Technology to confirm that these precautions are followed to ensure the security of and appropriate access to each data classification.

Data Classification

The County of Sacramento shall identify data according to the following classifications, based on the definitions contained in the California Statewide Information Management Manual section 5305-A.

A. Public data include information maintained by County departments that are not exempt from disclosure under the provisions of the Government Code sections 6250-6265 (California Public Records Act) or other applicable federal, state, or local laws. This applies to all business and financial data maintained by all County departments. With respect to County information and data, the presumption will be in favor of openness to the extent permitted by the law and subject to valid privacy, confidentiality, security, or other restrictions and exceptions afforded under the law. Examples of public data include:

    a. Basic Parcel Information (Situs Address, Tax Rate Area, Lot Size)
    b. Zoning and general plan land use maps
    c. Food facility inspection results
    d. Business license information
    e. Annual County budgets

B. Confidential data include information maintained by County departments that are exempt from disclosure under the provisions of the California Public Records Act or have restrictions on disclosure in accordance with other applicable state or federal laws. Examples of confidential data include:

    a. Personnel records including employee performance evaluations
    b. Medical files
    c. Investigatory records used for law enforcement
    d. Home addresses and phone numbers of County elected officials and employees
    e. Scoring keys to examinations for employment

C. Sensitive and personal information, as defined below, may occur in public or confidential data. Department Directors may further classify public or confidential data as containing sensitive and/or personal information.

    Sensitive information includes information maintained by County departments that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss or deletion. Sensitive data may be either public or confidential. Examples of sensitive data include:

    a. Water distribution and production infrastructure
    b. Sewer treatment plant infrastructure
    c. County financial transactions
    d. Contact information for citizens who place 311 Service Requests

D. All personal information must be protected from inappropriate access, use, or disclosure. Personal information includes information that identifies or describes an individual as defined in, but not limited by, the statutes listed below.

   a. Personally identifiable information (PII) includes any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, or employment information per National Institute of Standards and Technology (NIST) Special Publication 800-122.

   b. Protected health information (PHI) includes individually identifiable health information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to the entities in electronic or physical form. State law requires special precautions to protect from unauthorized use, access or disclosure. See Confidentiality of Medical Information Act, California Civil Code section 56 et seq., and the Patient Access to Health Records Act, California Health and Safety Code section 123100-123149.5.

   c. Electronic protected health information includes individually identifiable information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers that conduct electronic transactions to ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure. See Health Insurance Portability and Accountability Act (HIPAA), 45 Code of Federal Regulations parts 160 and 164.

   d. Personal information for research purposes includes information requested by researchers specifically for research purposes.

Access to Data

A. The public may request access to County data over the phone, at the public counter, by mail and online. Each department is responsible for responding to public data requests in accordance with the California Public Records Act and may provide public records that are not exempt from disclosure, containing requested data in hard copy or electronic format, subject to the requirements of the Act.

    a. Confidential data and sensitive or personal information contained within public data will be protected from inappropriate disclosure. If confidential data or sensitive or personal information is included in a public record, the department providing the public record will follow internal departmental procedures for removing or redacting the confidential, sensitive or personal information prior to releasing or disclosing the record.

B. Commonly requested public data, that does not contain sensitive or personal information, will be provided online through the County open data portal. Data sets included on the open data portal will be published using open standards and will be available online to the public without royalty or fee. The County will publish a description of what is contained in each of the data sets and information which will help the public access the data (metadata). Once published, these data sets will be periodically updated as information changes. Each Department Director is responsible for determining the department data sources that are public record and should be published on the open data portal.

C. Access to confidential, sensitive, or personal data is restricted to only those so authorized by law or County policy.

5. Review:

Biennially

6. References:

- California Statewide Information Management Manual (SIMM) section 5305-A
- California Public Records Act (CPRA), California Government Code section 6250 et seq.
- National Institute of Standards and Technology (NIST) Special Publication 800-122.

- Confidentiality of Medical Information Act, California Civil Code section 56 et seq.
- Patient Access to Health Records Act, California Health and Safety Code section 123100-123149.5
- Health Insurance Portability and Accountability Act (HIPAA), 45 C.F. R. parts 160 and 164