RESOLUTION
NO. 23 - 37

THE BOARD OF COUNTY COMMISSIONERS
OF HUERFANO COUNTY, COLORADO

A RESOLUTION TO ADOPT A POLICY FOR THE PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

WHEREAS, Huerfano County is required, under C.R.S. § 24-73-101 et seq., to implement and maintain reasonable security measures and practices that are appropriate to protect personally identifiable information ("PII") that the County may collect during the course of business; and,

WHEREAS, 2 CFR 200.303(e) requires the County to take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designates as sensitive or that the County considers sensitive consistent with applicable Federal, State, local, and tribal laws regarding privacy and responsibility over confidentiality; and,

WHEREAS, Failure to have a protection of PII policy could lead to fraud exposure and/or a breach of security for confidential information; and,

WHEREAS, the Board of County Commissioners desires the adoption of a policy for the protection of PII received by the County.

NOW, THEREFORE, BE IT RESOLVED by the Board of County Commissioners of Huerfano County, Colorado as follows:

Section 1. Title.
This resolution shall be known and referred to as the "Huerfano County Data Privacy Protection Policy"

Section 2. Policy, Purpose, and Scope

1. It is the policy of Huerfano County to protect personally identifiable information ("PII") to the maximum extent allowable pursuant to federal and state law, and to cause contractors, service providers, sub-grantees or other entities providing services to Huerfano County to do the same.
2. The purpose of this policy is to provide consistent guidelines for how the County deals with PII and Pl in regard to appropriate gathering of paper and electronic data, how long that data remains in the possession of the County if not controlled by other law or expectation, and how that data is disposed when no longer needed or retained as required by superseding regulation. This policy also outlines what notifications need to take place in the event of a data breach of Pl pursuant to C.R.S. § 24-73-103.
3. This policy applies to Huerfano County staff, contractor or service provider staff, sub-grantees or any other person involved in the handling of PII.

Section 3. Definitions.

1. **Personal Identifying Information (PII)** is a superset of personal confidential data defined as any of the following data elements:
    a. Social Security Number;
    b. Personal Identification Number;
    c. Password;
    d. Pass Code;
    e. Official state or government-issued driver's license or identification card number
    f. Government passport number;
    g. Biometric data (unique data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when
    h. accessing an online account);
    i. Employer, student, or military identification number; and
    j. Financial transaction device (any instrument or device such as a credit card,
    k. banking card, debit card, electronic fund transfer card, guaranteed check card, or account number representing a financial account).
2. **Personal Information (Pl)** is a subset of PII defined as:
    a. A Colorado resident's first name or initial and last name in combination with any one or more of the following data elements if not encrypted, redacted, or secured by a means to render the name of the element unreadable or unusable that would, for example, permit access to an online account:
        i. Social Security number;
        ii. Student, military, or passport identification number;
        iii. Driver's license number or identification card number;
        iv. Medical information (any information regarding medical or mental health
        v. treatment or diagnosis by a healthcare professional);
        vi. Health insurance identification number; or
        vii. Biometric data.
    b. A Colorado resident's username or email-address, in combination with a password or security questions and answers that would permit access to an online account; or
    c. A Colorado resident's account or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.
    d. Pl does not include publicly available information that is lawfully made available to the general public from federal, state, or local government record or distributed media.
3. **Retention**: Refers to the time when data that is in a readable or usable format is in possession of County services or vendors/contractors. For example, a "retention schedule" outlines, for a specific set of data, when data records are to be disposed of.
4. **Disposal**: Refers to the arrangement or destruction of data by shredding, erasing, or otherwise modifying the PII unreadable or indecipherable through any means.

5. **Notification**: The procedure of realizing when a security breach occurs, identifying the type of data affected and the set of Colorado residents it affects, and making required notifications to affected Colorado residents as well as notification to the Colorado Attorney General.
6. **Security Breach or Data Breach**: The unauthorized acquisition of unencrypted computerized data or physical records that compromise the security, confidentiality or integrity of Pl. This applies to the physical removal of paper records as well as, for example, a hard drive with data not effectively destroyed.
7. **Data Subject**: The person whose PII is being collected.
8. **User**: Any County employee or employee of a vendor, contractor, service provider, or sub-grantee who interacts with PII collected for County business in any manner during the course of their employment.

Section 4. Responsibility.

Data security is the responsibility of the individual dealing with PII, the office, service area, department, or division in which they operate, and the supporting security framework at the County administered by Huerfano County Information Technology ("HCIT"). Offices, service areas, departments, and divisions should carefully determine if this information is critical to collect, and if it must be collected, have effective measures to control and keep this information confidential, and effectively dispose of it when no longer needed or required. Offices, service areas, departments, and divisions are also responsible for ensuring vendors/contractors who maintain PII comply with this Policy.

1. Elected Officials shall be responsible for the general administration and implementation of a record retention schedule for their respective offices as determined appropriate by the Elected Official alone or in conjunction with the Colorado State Archives requirements. Elected Officials, or a designee thereof, shall act as the responsible authority within their office for ensuring departmental compliance relating to the retention and disposal of PII.
2. Department Heads shall be responsible for the general administration and implementation of a record retention schedule as adopted by the Board of County Commissioners and shall act as the responsible authority for ensuring departmental compliance relating to the retention and disposal of PII.
3. Each Department and Office shall ensure compliance with this Policy and make every effort to identify PII and how it relates to the intent of this Policy with respect to retention and disposal. They are also responsible for carrying out the external notification process, as directed by HCIT and the County Attorney, in the event of a data security breach that affects Pl.
4. HCIT, as part of its cybersecurity responsibility, will implement and maintain reasonable security procedures and practices to ensure that electronic data that has been identified as PII are adequately protected.
5. Offices, service areas, departments, and divisions are accountable to ensure vendor/contractors compliance to this Policy.
6. Users who collect PII during the course of business shall be responsible for compliance with this Policy and respective retention schedules, notifying department heads or elected officials of any suspected data breach, and carrying out any data disposal as appropriate to their job function.
7. Users will insure sharing PII will only be done using appropriate tools and procedures as defined by federal regulations, Colorado State Statute, and County

regulations, such as using approved encrypted email and secure file sharing services. PII is not to be shared informally outside of these tools and procedures.

Section 5. Procedures.

This section outlines the baseline requirements that responsible entities must follow in order to protect PII:

1. The County and employees, contractors, service providers, sub-grantees, or other affiliated entities should not collect PI or PII unless required as a function of mandate or service delivery.
2. To ensure that PII is not transmitted to unauthorized persons, all PII and sensitive data transmitted via email or stored electronically must be encrypted using industry-standard information processing standards. No user may email unencrypted PII to any entity.
3. All users must ensure that all PII is stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processes using County (or related contractor or service provider) equipment and information technology, at approved designated locations. Personal Electronic Devices will not be used to process PII.
4. Records/documents containing PII may not be left open and un-attended, will be stored in reasonable secure areas including locked rooms or cabinets, and users handling PII as part of their official duties will treat such documents as confidential.
5. Users who have access to PII will be advised of the confidential nature of the PII, the safeguards required to protect the PII and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal law.
6. Contractors, service providers, sub-grantees and others must have policies and procedures in place under which their employees and other personnel acknowledge the confidential nature of PII and the safeguards with which they must comply.
7. Contractors and service providers must not extract information from data supplied for any purpose not stated in the agreement, task order, grant, or other instrument governing their work with Huerfano County.
8. Access to PII created by the County must be restricted to only those users who need such information to perform duties in their official capacity.
9. All PII data must be processed in a manner that will protect the confidentiality of the records/documents and is designed to prevent the unauthorized dissemination of such records/documents by electronic or other means.
10. Records/documents that constitute official public records may be released pursuant to a public records request following procedures outlined in Colorado law and County policy.
11. PII should only be kept as long as needed or required by superseding regulations. Each office, service area, department, and division is responsible for identifying all physical or electronic records that contain PII and create a process for managing this information for appropriate use, visibility, and disposal.
12. Data should be regularly reviewed against the applicable records retention schedule. If no longer needed or required by state or federal law or regulation, data should be promptly and appropriately disposed.
13. Appropriate methods of destroying PII will be used by the County and its contractors or service providers when records are eligible for destruction pursuant

to applicable records retention laws and destroyed. Such methods may include shredding, burning, or electronically deleting PII.

14. If an office, service area, department, or division becomes aware of a potential data breach of records that contain Pl, it is required to take appropriate action as defined in this section to investigate the cause and extent of the breach. The office, service area, department, or division will work in conjunction with other departments including HCIT, the Sheriff's Office, and County Attorney to launch and manage such an investigation. If the investigation determines that there is sufficient evidence to conclude that a security breach involves the misuse or reasonable likelihood of misuse of Pl, HCIT and the County Attorney will work with the affected office, service area, department, or division to issue appropriate notices.
15. Failure by any user to comply with these requirements will result in disciplinary action up to and including termination of service agreements or employment at the discretion of the appropriate elected official or the Board of County Commissioners on the advice of HCIT, the County Attorney, or the County Administrator.

INTRODUCED, READ, APPROVED AND ADOPTED ON THIS 12th day of SEPTEMBER 2023.

BOARD OF COUNTY COMMISSIONERS
OF HUERFANO COUNTY, COLORADO

BY_____
John Galusha, Chairman

ATTEST:

_____
Arica Andreatta, Commissioner

_____
County Clerk and Recorder and
Ex-Officio Clerk to said Board

_____
Karl Sporleder, Commissioner